EUROPEAN
COMMISSION

Brussels, 27.11.2013
SWD(2013) 488 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Communication from the European Commission to the European Parliament and the Council on a European Terrorist Financing Tracking System (TFTS)

{COM(2013) 842 final}
{SWD(2013) 489 final}

Table of Contents

I. Introduction

When approving, in July 2010, the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Financing Tracking Program (EU-US TFTP Agreement), the Council called upon the Commission to submit a legal and technical framework for extraction of data on EU territory[1]. Likewise the European Parliament asked at various occasions to envisage a durable, legally sound European solution regarding the extraction of requested data on European soil[2]. Article 11 of the EU-US TFTP Agreement states that during the course of that Agreement the European Commission will carry out a study into the possible introduction of an equivalent system allowing for a more targeted transfer of data than encompassed in that Agreement.

In "The Stockholm Programme - An open and secure Europe serving and protecting citizens"[3], the Council called upon the Commission to examine the possibilities to track terrorist financing within the Union.

In its Communication of 22 November 2010 to the European Parliament and the Council "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe"[4], the Commission committed itself following the signature of the Terrorist Financing Tracking Programme agreement with the United States to examine the possibility of developing a policy for the EU to extract and analyse financial messaging data held on its own territory.

As a first stage of its response to these calls and the contents of Article 11 of the EU-US TFTP Agreement, the European Commission published a Communication to the European Parliament and the Council "A European terrorist financing tracking programme: Available options"[5] on 13 July 2011. The purpose of the Communication was to present different options regarding the introduction of a European TFTS and the points to take into consideration with respect to these options. It did not name a preferred option but rather intended to trigger a debate on the part of the Council and European Parliament given the political importance of the issue and its legal and technical complexity.

Based on the subsequent discussions and a comprehensive study carried out by an external contractor, the European Commission has completed this Impact Assessment. By doing so, it has in particular looked into the impact of a possible legislative proposal in this context on fundamental rights, and especially on data protection. Specific attention was paid to the necessity and proportionality of any measure. In addition, the Impact Assessment takes particular account of the financial burden for the EU, for Member States and for Designated Providers of the data in question which the introduction of a new system would cause. Moreover, based on the Commission report on the second joint review of the EU-US TFTP agreement[6], developments as well as statistical information regarding the actual application of the Agreement by Member States, in particular its Articles on reciprocity (Art. 9 and 10), have carefully been taken into account.

[1] Council Decision of 13 July 2010, OJ L 195, 27.7.2010, p.3
[2] See, for example, Resolution TA(2010)0143
[3] OJ C 115, 4.5.2010, p.1
[4] COM(2010)673 Final
[5] COM(2011)429 Final
[6] SWD(2012) 454 final of 14.12.2012

II. Procedural Issues and Consultation of stakeholders

II.1 Procedural issues

The preparation of this impact assessment has involved close coordination across Commission services. An Inter Service Group on the establishment of an EU system equivalent to the Terrorist Finance Tracking Programme (EU TFTS) was set up in November 2010 to inform on the state of play of the implementation of the EU US TFTP agreement, on the expert meetings referred to below and the state of play of the preparatory study that DG HOME commissioned but most importantly to discuss the preparation of the impact assessment. The ISG comprised the following services: HOME, JUST, SG, SJ, EEAS, HR, INFSO, OLAF, MARKT. The ISG met on 7 occasions.

Work on the IA began in April 2012 and has been conducted over a period of six months. The IA was submitted to the Impact Assessment Board (IAB) on 19 September and discussed on 17 October. The Minutes of the last ISG meeting were submitted to the IAB.

The IAB's recommendations from its opinion of 19.10.2012 have been fully taken into account and have led to various amendments in the impact assessment, in particular as concerns the problem definition, the baseline scenario, the options and their assessments and the presentation of the stakeholder views.

On 30 April 2013 the Board issued an overall positive opinion on the Impact Assessment and put forward a number of suggestions for further improvements which have been accommodated to the extent possible in this final version of the Impact Assessment,

II.2. External expertise and consultation of stakeholders

The Commission services have made substantial efforts to obtain evidence in this field and to ensure full engagement of the different stakeholders:

- In December 2010, GHK Consulting Ltd (GHK) was commissioned by the Commission Services to undertake a preparatory study to inform the impact assessment of a European System equivalent to the existing US Terrorist Financing Tracking System. The contract was extended, from a total duration of 7 months to a total duration of 14 months for two major reasons: 1.) to ensure that the study could cover other policy options than those examined so far by the study, which might also come out of the discussions with the Council and the European Parliament following the Communication of 13.07.2011 and 2.) to allow for sufficient time for a more thorough analysis and refinement of certain elements, including fundamental rights issues and the overall market of financial messaging services. The study was finalised in April 2012 and involved an extensive consultation of various stakeholders[7].

- In order to discuss the possible creation of an EU TFTS system and its implications as well as links to the EU-US TFTP agreement and possible impact on this, the Commission Services carried out four expert meetings from November 2010 to April 2011 involving stakeholders such as EUROPOL, European Data Protection Supervisor (EDPS), the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and many Member State experts (representing relevant ministries, law enforcement/ intelligence agencies and DPAs). Experts from the US Treasury Department participated at parts of one meeting to report on the US Terrorist Financing Tracking Programme.

- On 24 November 2010, the meeting focused on the roles of SWIFT and Europol under the existing EU-US TFTP Agreement.

[7] Among the consulted stakeholders were representatives from the US Treasury, Europol, FIU.net, EEAS, SWIFT, EDPS as well as experts from various MS' authorities.

- The Meeting on 21 January 2011 addressed the functioning of the US TFTP system and data protection aspects of a potential EU equivalent.

- The Meeting on14 March 2011 focused on questions related to the interpretation and implementation of the EU-US TFTP Agreement.

- Finally, the meeting on 14th April 2011 was used to present and discuss draft policy options.

The Commission Communication of July 2011 on the state of play and possible options received only limited feedback.

In the Council, the issue was discussed at various occasions in a number of Council Committees and by the JHA Ministers on 27 October 2011. While it is important to note that Ministers only presented preliminary views and reserved their final positions, it can be taken from this ministerial debate that a great number of Member States (1) stressed the need for an in-depth analysis of the costs occurred by any new system, (2) emphasised that a new system should not undermine the existing agreement with the US and (3) could not agree on any of the options presented by the Commission in its Communication of July 2011. Whereas some Member States noted the added-value of an EU internal system, a considerable number of Member States was much more sceptical. The need to take full account of data protection rules was highlighted by a great number of Member States.

The European Parliament, by contrast, never formally reacted to the Commission's Communication of July 2011. It did not decide to nominate a rapporteur for the issue. The LIBE committee discussed the issue, albeit briefly, at a meeting in autumn 2011. In addition, on 6 November 2012 the Director-General of DG HOME met with the LIBE coordinators to discuss the EU TFTS and to update on the state of play of the Impact Assessment. The views expressed by the different political groups showed that, on a personal basis, some MEP's from three of these groups strongly opposed the options included in the Commission's Communication and proposed another way to address the issue, i.e. by data retention and extraction. This is the reason why the current Impact Assessment addresses more than those options detailed in the July 2011 Communication in order to make sure that all (even if only remotely) politically relevant options are carefully analysed in this Impact Assessment. The additional options are listed as options B.4.1 and B.4.2. To complete the picture of possible options, the Commission decided to include an option called "status quo plus". This option, listed as option A.2, builds upon the status quo of the current application of the EU-US TFTP Agreement but would include certain amendments to this Agreement to better reflect EU specific issues.

Finally, the Commission also received some limited feedback from citizens but also from one national Parliament. Most of this feedback highlighted the need to protect the fundamental rights of those affected by any new instrument, including the right to personal data protection. In addition, the Article 29 Data Protection Working Party stressed that the Commission would first need to make the case as regards the legality and necessity of a new TFTS before a detailed analysis regarding the data protection implications could be made. It also emphasised, amongst others, the need to include a careful definition of the data that will be processed, ensure that the data processed would meet the necessity test and that sufficient safeguards would be applied by all authorities involved.

Given the technical complexity of the questions at stake and their operational and political sensitivity because of their impact on security and relations to a third country a more extensive general public consultation was not carried out.

III. Policy context, problem definition and the EU's right to act

Policy context	Problem definition	Drivers – Current Key Problems
Terrorism remains a major threat to the security of EU citizens and property	Terrorism and its financing are mainly transnational in nature Existing instruments/ measures are inadequate for tracking the financial trail of terrorists activities in Europe	The current mechanism in place to analyse financial messaging data is run by a third country and requires the transfer of large amounts of such data from the EU to that third-country. While Member States as well as Europol/Eurojust can benefit from the current mechanism through reciprocity clauses, the mechanism logically does not fully represent EU interests.
		The current mechanism in place to analyse financial messaging data only covers one financial messaging provider and one type of message
		Despite its ratification by EP/Council, a number of safeguards and joint reviews confirming their proper application, the current mechanism in place to analyse financial messaging data raises questions as to the level of protection of privacy and personal data of European citizens.
		There is insufficient technical and legal capability within the EU/ MS to establish financial linkages to trace and map terrorist networks apart from information obtained through the TFTP Agreement.

III. 1 Policy context

Terrorism remains a major threat to the security of EU citizens and property

Europol's TE-SAT report 2010[8] included statistics on trends and stated that 1,359 terrorist attacks were carried out in the EU between 2007 and 2009 by separatists; a further 104 attacks were carried out by left-wing terrorism; and 4 attacks by Islamists. Europol's TE-SAT 2011 report[9] indicates that, in 2010, in 9 Member States, 249 terrorist attacks were completed, failed or foiled, of which 160 as part of separatist terrorism, 45 by left-wing terrorism and 3 by Islamist affiliations. The total number of arrests in that same year amounted to 611, mostly of separatists (349), followed by Islamist terrorists (179). A total of 307 persons stood trial for terrorist charges in 11 Member States, with Spain by far having the highest numbers of trials, namely 173. In 2011, a total number of 332 persons were convicted (241) or acquitted (91) for terrorism charges, again with the highest number in Spain (198, with 122 convictions and 76 acquittals). Finally, Europol's TE-SAT 2012 report indicates that, in 2011, in 7 Member States, 174 terrorist attacks were completed, failed or foiled, of which 110 as part of separatist terrorism, 37 by left-wing terrorism, and one by right-wing terrorism (27 not specified). The total number of arrests in that same year amounted to 484, mostly of separatists (247), followed by religiously inspired terrorists (122). A total of 316 persons stood trial for terrorist charges in 11 Member States. A total number of 332 persons were convicted (241) or acquitted (91) for terrorism charges.

Member States continue to be exposed to a serious threat from religiously inspired/Islamist, ethno-nationalist and separatist, as well as from left–wing and anarchist terrorism. The scale of terrorist attacks varies greatly between the Member States. In the past, some Member States experienced and/or prevented several Islamist attacks such as Spain, the Netherlands and the United Kingdom. Member States also suffered from anarchist, left-wing or separatist terrorism (e.g. France, Greece, Denmark, Italy and Spain) or from right-wing terrorism. The threat level in the Member States ranges between very likely, likely or moderate, with most threat expected from Islamist groupings. EU citizens are victims of terrorism all around the world, not just in Europe. For example, six EU citizens lost their lives and 15 were injured in the 2008 Mumbai terror attacks.

Europol confirms that while the number of terrorist incidents and arrests in Europe may continue to fall, overall activity relating to terrorism still represents a significant threat to EU Member States (TE-SAT 2012 Report).

Obviously there are more important impacts related to terrorism than economic ones, above all when human lives are affected. However, at this point, it should also be mentioned that terrorism has direct and indirect effects on the economy. The direct economic effects and consequences of terrorist attacks include loss of life and loss of productive capacity of those killed, injured or traumatised; destruction of physical property and infrastructure; responses to the emergency, restoration of the systems and the infrastructure affected, and the provision of temporary living assistance. The immediate material damages of the Madrid bombings were estimated at € 17.62 million, and minimum direct economic cost has been estimated at more

[8] The Europol EU Terrorism Situation and Trend Report 2010 (TE–SAT). Available at: http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/Tesat2010.pdf

than € 211.58 million[10]. The indirect costs of terrorism are often even more significant and have the potential to affect the economy in the medium to long term, for example by undermining consumer and investor confidence; abnormal losses suffered by certain directly impacted industries, sectors, localities or regions; increased costs of security analogous to a 'security' or 'terrorist tax'; opportunity cost of spending additional money to fight terrorism and other long-run costs. A number of studies have been conducted which attempted to quantify the overall cost of a terrorist attack[11]; some of these focused on the impact of 9/11. A dedicated OECD Report of 2002 focused on the economic consequences of 9/11.

Terrorist financing is the financial support in any form, of terrorism or of those who encourage, plan, or engage in terrorism. Countering the financing of terrorism means to prevent terrorists and entities linked to terrorism from collecting, moving and gaining access to funds and by this to deprive terrorists from their possibility to engage in terrorist activity. That is why countering the financing of terrorism is a core component of the EU's strategy and fight against terrorism.

The EU's Counter-terrorism strategy stresses that tackling terrorist financing is part of creating a hostile operating environment for terrorists[12]. The EU's revised Strategy on Terrorist Financing of 17 July 2008[13] points out that efforts have to be maintained to prevent terrorist financing and control the use by suspected terrorists of their own financial resources. The explicit mentions in the EU's Stockholm Programme and the Commission's Internal Security Strategy have been referred to above. This policy is completely coherent with other relevant EU initiatives and legislation, in particular

- Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing which imposes, for example, obligations on financial institutions and other stakeholders to report suspicious transactions related to terrorist financing. In February 2013, the Commission has published a proposal[14] to review this Directive in order to up-date it and to adapt it to the revision of international standards.

- Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds which aims at preventing terrorists from having unfettered access to wire transfers.

- Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community which has the objective to hinder terrorists and others from smuggling money in cash across borders.

- Regulation (EC) 2580/2001 freezing funds of suspected terrorists and Regulation (EC) 881/2002 implementing UN Al Qai'da and Taliban sanctions which by preventative means deprive terrorists from making use of their financial assets.

[10] The economic costs of March 11: Measuring the direct economic costs of the terrorist attacks on March 11, 2004 in Madrid (Mikel Buesa, Aurelia Valino, Joost Theijs, Thomas Baumert and Javier Gonzalez Gomez)
[11] Economic Impacts of Global Terrorism: From Munich to Bali (2006, Barth, J.R., T. Li, D. McCarthy, T. Phumiwasana, and G.Yago)
The Economic Analysis of Terrorism (2007, Bruck, T.)
[12] 14469/4/05 REV of 30 November 2005.
[13] 11778/1/08 REV 1
[14] COM(2013) 45 final.

III.2 Problem definition

III.2.1 The transnational nature of terrorism and its financing make detection and acting against terrorism funding very challenging

Most terrorist activities are transnational in character and involve fund raising and transfers which cross borders. Terrorist organisations are highly pragmatic in their approach to financing their activities. Political boundaries are easily ignored if they stand in the way of the acquisition of funds[15]. It is not unusual at all that funds are collected or generated in one country and then transferred to another country be it to spend it for the preparation of and purchase of goods for the actual terrorist attack on the ground, to subsidy a local terrorist network or training camp etc. There have been cases, for example, where an allegedly charitable association collected donations in a Member State to transfer the money then to a third country for the purchase of arms which then were employed in the Near East.

Because of its transnational nature, detecting and stopping the financing of terrorism is extremely challenging. By crossing borders with their funds, terrorists try to cover up their tracks and to benefit from different jurisdictions with unequal levels of surveillance and control. International cooperation in this field is therefore of utmost importance. That is why the EU and the US agreed to work closely together in this field, as demonstrated in particular by the EU US-TFTP agreement. The US is a key strategic partner for the EU in the fight against terrorism and its financing but apart from the US, the EU also maintains good counter-terrorism co-operation with other countries around the globe.

At international, EU and national levels, Member States have different instruments and measures at their disposal to identify and combat the financing of terrorism. Important EU instruments are the Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and the Council Decision concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. There are other legal instruments impacting the issue of terrorist financing such as Council Regulation on specific restrictive measures directed against persons and entities with a view to combating terrorism, Regulation on information on the payer accompanying transfers of funds or Regulation on controls of cash entering or leaving the community, nevertheless the primary objective of these instruments is not to provide and exchange pertinent intelligence information.

In existing legislation terrorism financing is often put in context with organised crime, in particular money laundering. This was reflected in the preparation of the current Impact Assessment by the wish of some stakeholders and Member States to also consider whether data gathered by a new EU TFTS could also be used for purposes beyond fighting terrorism, namely fighting serious organised crime. That is why particular consideration is given to the purpose of a new system and why specific options address it in this assessment.

At the same time, there is a body of EU legislation to ensure that personal data obtained and processed by the EU or the Member States is adequately protected from unauthorised access and misuse, and treated with respect for the fundamental rights in relation to privacy (Article

[15] Europol TE-SAT 2012 Report

7 of the Charter of Fundamental Rights) and data protection (Article 8 of the Charter of Fundamental Rights). In addition to various legislative instruments, there are also a number of international and EU bodies which are actively involved in the fight against terrorist financing, such as the Financial Action Task Force on Money Laundering and Terrorist Financing (FATF), the Committee on the Prevention of Money Laundering and Terrorist Financing, the EU Financial Intelligence Units (FIU) Platform, Eurojust and Europol.

III.2.2 Existing instruments/ measures are inadequate for tracking the financial trail of terrorists

Even if cooperation between Member States is increasing, for example at the level of the FIUs, or as part of EUROPOL and Eurojust, the combating of terrorism has mainly remained a national matter. Within each Member State, national law enforcement authorities can obtain direct information, via judicial or extra-judicial channels. However, given that terrorism is a global phenomenon, investigations often require the collection of information and evidence across borders. For this, Member States can make use of a series of instruments, such as, for example, bilateral co-operation, Mutual Legal Assistance (MLA) and, within the EU, the European Evidence Warrant (EEW). However, obtaining information from third countries is often much more complicated, time-consuming or sometimes even impossible in practice. This is also the case when MLA instruments exist. For example, there may be reliable information that a specific terrorist is moving money from Africa to Europe or elsewhere in preparation of a terrorist act but the banks to which he or she is sending the money or even the countries in which those banks are located may not be known. It would be impossible for the country concerned to issue MLA requests for the relevant records of every bank in every country in the EU or elsewhere in the world.

FIUs, especially through FIU.NET, a decentralised computer network for the exchange of information between FIUs, and as part of their general cooperation and information exchange activities, already have a much greater capacity to track financial transactions. However, in most cases they can only take the initiative following suspicious transaction reports. Furthermore these reports are not very frequent in the context of terrorist financing as reporting entities, like financial institutions, have difficulties in identifying the terrorist context since, contrary to money launderers, terrorists and those financing terrorism often use legal money for their purposes.

After 9/11, the United States have decided to tackle the problem of terrorist financing more effectively by setting up a Terrorist Financing Tracking Program (TFTP) which aims at analysing international bank transfers of certain types and from certain geographical regions. In order to have access to relevant financial data stored in the EU, the US has concluded an agreement with the EU, the EU-US TFTP Agreement.

III.3 Problem drivers

III.3.1 Driver 1: The current mechanism in place to analyse financial messaging data is led by a third country, thus not fully representing EU's specific interests.

As stated above, Europol and other sources confirm that the threat of terrorist attacks remains significant.

In the EU, the threat comes mainly from separatist, religiously inspired, left-wing and anarchist terrorists, which appear to be 'cyclical' in terms of their intensity and risk they represent and, to some extent, quite different from the threat to the US. The threat in the latter mainly comes from Islamist terrorism, which does not have, or only has a limited, presence in the US itself. This implies that the TFTP has been mainly used by the US for the purpose of investigating terrorist activity linked to the threat as perceived by the US, and less on forms of terrorism which pose a threat to the EU.

In the past Member States made relatively little use of the reciprocity clauses contained in the EU-US TFTP agreement and hardly benefitted from the data exchange themselves, mainly due to a lack of awareness. This, however, has changed in the period addressed in the second review (March 2011 to September 2012) as the Commission confirms in its second joint review report regarding the implementation of the EU- US TFTP Agreement[16]. This report demonstrates that Member States are increasingly applying the reciprocity clauses in this Agreement to benefit themselves from the data exchanged with the US. This shows that this problem driver cannot be seen as a static one but as the EU-US TFTP Agreement has been further applied and all actors are in the process of constantly gaining more experience with it, the importance of this problem driver has decreased over time.

III.3.2 Driver 2: The current mechanism in place to analyse financial messaging data only covers one financial messaging provider and one type of message

Given that it is a US programme with a global focus, at present, only FIN messages (Financial Institution Transfer messages) transferred through the SWIFT network are included in the TFTP. FIN messages are a SWIFT created message type by which financial information is transmitted from one financial institution to another. According to SWIFT, FIN is their core messaging system that enables over 8.300 financial institutions in more than 200 countries to exchange financial data securely. The fact that the TFTP only covers this kind of messages, however, represents several limitations. First, whilst FIN covers part of the financial messaging "market", the competitive landscape is larger and divided over different types of services. This means that terrorists can make use of alternative financial channels. Although being the biggest global player, SWIFT still only handles a minor share of all money transfers in the world.

The Automated Clearing House (ACH) is another important electronic payment transfer system. Globally in 2009, 48% of all non-cash payments were processed through ACH (75 billion) and within the EU, 58% of all payments were processed through ACH (42 billion), mainly handling individual, equal currency, low value transactions (retail payments).

[16] SWD(2012) 454 final

Domestic non-Market Infrastructure payments (In-house) and Cross-border payments (Correspondent banking) also play an important role. These encompass transfers between banks, but outside payment systems for clearing and settlement and make up the second largest payment category, with an estimated global share of 42.5% and an EU share of 42%. In-house transactions are most often communicated via the banks' own communication tools.

Whilst the incidence of FIN messages in cross-border payments is high, it is also assumed that the largest remainder of such payments are handled through direct communication networks between the banks, with a relatively lower share being communicated through other proprietary networks competing with SWIFT.

Another important payment device is electronic money (e-money). Electronic money is a digital equivalent of cash, stored on an electronic device or remotely at a server. Payments made via e-money services were already estimated to represent 7.75% of the total global transactions and 5.5% of transactions in the EU. The by far largest player in the EU, PayPal, globally represented in 2009 21% of the market and 1.6% of all global transactions, with a share in the EU of 3.4% on all transactions and 63% on e-money payments. E-money services are growing rapidly.

Apart from that, other payment methods, such as those made via remittances services, exist.

III.3.3 Driver 3: The current mechanism in place to analyse financial messaging data raises concerns as to the protection of privacy and personal data of European citizens

Most criticism concerns the TFTP's alleged inconformity with the right to respect for private and family life (Article 7 of the Charter of Fundamental Rights) and the right to the protection of personal data (Article 8 of the Charter of Fundamental Rights and Article 16 of the TFEU), as well as with the obligations under the Data Protection Directive (Directive 95/46/EC) and other relevant EU Acquis. As stated above, similar concerns have also been expressed in relation to a possible future EU system, and were the major point of distress put forward in feedback to the Commission's Communication of July 2011. Concerns regarding the existing system referred amongst others to differences between US data protection legislation and EU legislation, as in the US the right to privacy is not an explicit fundamental (constitutional) right and as the US has a sectorial approach rather than a comprehensive set of data protection instruments. In addition, stakeholders also question the necessity and proportionality of transferring bulk data on EU citizens to a third country and criticise the verification and authorisation processes to allow for the transfer of such data.

The first joint review as well as the second joint review of the implementation of the EU-US TFTP Agreement by the Commission have verified that the comprehensive safeguards included in the Agreement, in particular those related to personal data protection, function properly. The practical and to date more experienced application of the EU-US TFTP Agreement has put this problem driver's relevance in the context showing that the original concerns at the time of initial analysis of an EU system have been addressed by the effective set of safeguards embedded in the Agreement.

III.3.4 Driver 4: Besides the EU-US TFTP Agreement, there is insufficient technical and legal capability within the EU and in Member States to establish financial linkages to trace and map terrorist networks

Within its limitations, the TFTP is the only mechanism which can map and profile those suspected of terrorism or financing terrorism, and show their financial movements and links, within a very short time period, requiring very few resources. By linking them in an objective way to suspected terrorists, the TFTP is capable of bringing previously unknown persons on the "radar screen" and, by doing so, supports law enforcement authorities dismantling terrorist networks and prevent further terrorist activities.

Whilst other existing instruments are able to provide some 'parts of the puzzle', none is able to do the same as a TFTP-like system. The system is unique in that it allows access to financial messages from all financial institutions using the FIN messaging service, i.e. potentially covering more than 9,000 financial institutions in 209 countries. It is therefore able to address the global nature of terrorism.

At the level of the EU, there is no equivalent system in place which would disclose financial linkages to trace and map terrorist networks. The existing legislative and operational instruments which have been set up at the level of the EU and Member States or in which the EU and Member States participate (like the FIU.net, co-operation between EU FIUs be it bilaterally or in the context of the FIU platform, mutual legal assistance instruments) do not, cannot and have not been created to offer the same advantages as the TFTP in terms of speed, efficiency and effectiveness. Pursuant to the preventive system based on the 3rd Anti-Money Laundering Directive, for example, Financial Intelligence Units analyse financial transactions on a case by case basis following suspicious transaction reports by obliged entities such as financial institutions. The EU freezing system related to terrorist funds requires a formal list of persons and entities related to terrorism agreed by the Council in order to prevent financial transactions of those listed. But there is no system in place that uses data which would make it able to show a complete pattern of financial "behaviour" and connections of a person or organisation suspected of terrorism or financing terrorism.

III.4 Baseline scenario - How will the problem evolve without action?

The international cooperation and the capability of Member States to trace and map terrorist will remain important in light of the persisting threat of terrorist attacks.

Under the baseline scenario, no EU TFTS system would be created at this stage. The EU US TFTP Agreement would continue to exist and to be applied. There would be one Designated Provider being obliged to disclose relevant financial data and only its FIN messages would be covered. There would not be any additional costs for Member States or the EU which the establishment of a new system would cause. Moreover, no additional data, including personal, would be collected.

Member States, Europol and Eurojust would continue having a possibility to use the TFTP within its limitations as described earlier. Reciprocity is a basic principle underlying the EU US TFTP Agreement and two provisions (Articles 9 and 10) are the basis for Member States as well as, where appropriate, Europol and Eurojust to benefit from TFTP data. These provisions enable EU authorities to obtain directly relevant financial data from the U.S. Treasury which helps them to fight terrorism and its financing more efficiently in the EU.

Article 10 stipulates that a law enforcement, public security, or counter terrorism authority of a Member State, or Europol or Eurojust, may request a search for relevant information obtained through the TFTP from the US if it determines that there is reason to believe that a person or entity has a nexus to terrorism or its financing. Pursuant to Art. 9 of the Agreement the U.S. Treasury Department shall ensure the availability to law enforcement, public security, or counter terrorism authorities of concerned Member States, and, as appropriate, to Europol and Eurojust of information obtained through the TFTP.

Member States hardly made any use of these rights shortly after the EU US-TFTP Agreement took effect. According to the second review of the application of the EU US TFTP Agreement, as reflected in the report by the Commission[17], Member States are increasingly making use of the reciprocity clauses contained in the Agreement in order to benefit from TFTP data for their fight against terrorism and its financing. The report shows that there were only ten Article 10 requests during the six-month period after entry into force of the EU US TFTP Agreement. However, there were 94 requests sent to the US in the period addressed in the second review. This figure only reflects those sent via Europol. The actual figure is presumingly higher as Article 10 allows Member States to send requests directly to the U.S. Treasury. One reason for this increase is a greater awareness of this mechanism on the part of Member States. Europol actively contributed to raising this awareness by promoting the reciprocity provisions through dedicated campaigns in Member States. Apart from that, the U.S. Treasury sends reports on possible terrorist threats to EU Member States and Europol without a specific request based on Art. 9 of the EU US TFTP Agreement.

These figures and insights gained during the second joint review of the EU-US TFTP agreement[18] show that the TFTP data exchange is no longer a "one-way street" but that Member States are using this programme increasingly for their own purposes to fight terrorism and its financing. There are no indications that the active use of the reciprocity clauses of the Agreement and consequently the benefit on the part of Member States and Europol with regard to TFTP data would diminish in the future.

In addition, the TFTP is equipped with robust control measures to ensure that safeguards, including those on personal data protection, are duly respected. Proper implementation of these safeguards has been subject to two joint reviews carried out in 2011 and 2012. Therefore, under the baseline scenario the current level of personal data protection would be maintained while, at the same time, also not increasing the amount of data collected.

In the course of the second joint review, Europol as well as Member States underlined the importance of data received via TFTP for their fight against terrorism. During the second joint review and despite the difficulties in declassifying information related to TFTP based investigations, the US Treasury showed various actual examples of cases in which TFTP based information supported the identification of terrorists or terrorist activities, including cases related to the EU. A number of such case examples have been annexed to the second joint review report following declassification by the US.

Furthermore, the US Treasury and Europol confirmed in the course of the second review that requests based on Article 10 of the Agreement are dealt with in short time. This was also confirmed by Member States' experts at a meeting in Brussels on 23 November 2012 which

[17] SWD(2012) 454 final of 14.12.2012

focussed especially on the reciprocity clauses. Member States confirmed that, while replies to their first requests based on reciprocity took some time to be answered by the US, there had been very positive developments and, by now, replies were received without any undue delay. This shows that as the reciprocity mechanism had been a new instrument in this context, it took some time to become known and fully operative.

III.5 EU's right to act and justification

The Commission, in Article 11 of the EU-US TFTP agreement, has been given the specific mandate to explore the introduction of an equivalent EU system, which should allow for a more targeted transfer of data. The right of the EU to act in this field is further enshrined in Article 82 and Article 87 of the Treaty on the Functioning of the European Union (TFEU).

The threat from terrorism remains significant and there are benefits of new and effective tools to prevent terrorist attacks and to map the movement of financial transactions to identify terrorists and those financing terrorism. Such tools should take account of the transnational nature of terrorism, crossing international borders and establishing cells in many different countries.

Article 67 of the TFEU stipulates that the EU shall constitute an area of freedom, security and justice and asks the Union to ensure a high level of security through measures to combat crime. For the introduction of a Terrorist Financing Tracking System to run searches of financial movements with the aim to detect links to terrorism across the Member States and third countries, the EU is best placed to take action. EU action would also guarantee the application of high common standards for the protection of personal data and additional necessary safeguards.

Need to act

The TFTP is U.S. intelligence tool, providing opportunities which at present do not exist on the EU territory. The system takes into account the global nature of terrorism and the commonly dispersed structure of terrorist organisations, broken down in cells which appear entirely unconnected and based in different EU and third countries spread over the world. The TFTP has proven to be a valuable tool for counter-terrorism investigations. This has been demonstrated in the context of the second joint review of the EU US TFTP Agreement. The report on this review contains in its Annex IV examples of recent terrorist cases illustrating the added value of the agreement. This set of examples relates to a number of terrorist groups including Al Qaida and Al-Shabaab and highlights some of the cases in which the TFTP has provided key leads as well as the ways in which TFTP derived data have helped to identify the financial support networks behind these terrorist groups currently under investigation by U.S. and European authorities. In particular, the case of the Islamic Jihad Union (IJU) underlines the concrete value of the system for EU Member States as it concerns the preparation of a serious terrorist attack in an EU Member State.

Without the TFTP, it would in several cases have been impossible to identify terrorists and their financial supporters through 'traditional' law enforcement and judicial instruments on time. In nearly all cases in which the system was used, they would not have been identified in such a short time period. The TFTP presents some huge efficiency gains and savings, both in terms of quality, time and resources, as it allows investigators to focus their efforts from the very start, through the provision of highly accurate and reliable information. In addition, EU

authorities are increasingly benefitting from TFTP data based on the application of the reciprocity clauses contained in the agreement as referred to above. However, TFTP presents still some limits, such as covering only one designated provider and one messaging system, which a proper EU system could mitigate in order to better achieve the objective of effectively fighting terrorism and its financing from an EU perspective and within the EU.

Subsidiarity

The issues to be addressed, i.e. the threat of terrorism and the huge social and economic costs of a terrorist attack, are of a transnational nature, affecting more than one Member State at the same time. In this sense, they cannot be dealt with in a fully satisfactory manner by the individual Member States. Only an EU-wide system would enable the co-operation needed between Member States to control and track the financial transaction taking place within the EU but also between the EU and third countries. National systems would inevitably be limited to track and check transactions with a domestic link and could consequently not provide the same level of security for the EU. Member States would need to cumbersomely compare each other's data which would render a system based on domestic programmes very slow and complicated.

Proportionality

By its nature, a TFTP like system requires the use and processing of bulk data which is privately held and collected by service providers for a different purpose than law enforcement. This means inevitably interference with the fundamental rights to the protection of private life and to the protection of personal data as recognised by Articles 7 and 8 of the Charter on Fundamental Rights of the European Union and Article 8 of the European Convention of Human Rights, as well as Article 16 of the Treaty on the Functioning of the European Union. These rights can be subject to limitations, as defined in Article 52 of the Charter on Fundamental Rights of the European Union, which allow for interferences that are "in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others", "in accordance with the law" and "necessary in a democratic society". The two Commission reports on the joint EU US Reviews of the TFTP agreement came to the conclusion that, with regard to the operation of the TFTP, rigid control measures were in place to ensure that safeguards, including those on personal data protection, were duly respected. This demonstrates that sufficient safeguards could be incorporated in such an instrument and be properly implemented thus ensuring its proportionality.

If EU action would consist of establishing an EU equivalent system, this would inevitably lead to the collection of personal data. It would need to be accompanied by a clear legal framework, based on relevant EU data protection legislation. Appropriate control measures and arrangements should be put in place and the data which is being processed would need to be carefully defined and limited to a minimum whilst still ensuring the functionality and the added-value of a new system.

In order to assess the proportionality of establishing a new system, the issue of additional impacts on Member States' and the EU's budget would also need to be taken account, in particular given the current economic situation and linked austerity programmes.

IV. Objectives

Terrorist offences cause severe harm to victims, inflict economic damage on a large scale and undermine the sense of security without which persons cannot exercise their freedom and individual rights effectively. The principal objective of an EU TFTS would be therefore to cut off terrorists' access to funding and to track financial transactions linked to terrorism in order to enhance security in the EU.

Outline of General, Specific and Operational Objectives		
General Objectives	**Specific Objectives**	**Operational Objectives**
To track terrorists' financial transactions in order to fight terrorism and to enhance security	1. To ensure that the system is tailored to respond to EU's intelligence requirements given its threat assessment	To improve the relevance and effectiveness of searches and analyses of financial messaging data. To increase Member State participation in and use of the financial messaging data
	2. To maintain effective cooperation with the US and other third countries in the fight against terrorism	To ensure data/ intelligence sharing between the US and EU is based on the principle of reciprocity To ensure that the EU/ Member States can share the results of relevant searches with other third countries
	3. To ensure that the analysis of financial messaging data covers the most relevant service provider(s) and message type(s)	To prevent terrorists from escaping the net
	4. To ensure full protection of the rights to privacy and data protection of European citizens when processing financial messaging data	To ensure data security and integrity To ensure that all processing activities will comply with current EU data protection law To put in place robust safeguards, oversight and control To provide citizens with appropriate administrative judicial protection, in terms of access to remedies and redress
	5. To increase the EU and Member State access and analyses of financial messaging data and their capacity to identify links between individuals/ groups involved in terrorism or its financing	To put in place an EU or Member State capability to analyse financial messaging data To improve efficiencies in the fight against terrorism by channelling and having an overview of financial information and data from all Member States To increase the investigative capabilities of the EU and Member states

V. Policy options

Policy Option	Description
A 'No EU TFTS' options	
A.1 Status quo (baseline)	This policy option involves no further/ new action being taken by the EU. Under this option, the present arrangements as per the US-EU TFTP Agreement would continue.
A.2 Status quo plus	Under this option, the US-EU TFTP Agreement would continue, but amendments would be made. These would ensure a higher EU involvement in the TFTP, for example by compiling requests for "raw" data in consultation with EUROPOL and/or the Member States and by allowing EUROPOL and/or Member State analysts to access the system, meaning that they could run searches autonomously. This would also require agreement by the US and a formal approval of the amendments by the EU legislator.
A.3 Zero option	This policy option involves the termination of the present US-EU TFTP Agreement, in the scenario that Member States / the EU would withdraw its support of the agreement.
B EU TFTS ***With various sub options*** ***for the structure***	
B1. Centralised system at EU level	**The EU TFTS**. This policy option would involve an EU legislative instrument establishing a fully centralised EU TFTS unit. The tasks and functions of the unit would be fully centralised, meaning that issuing requests for "raw" data to the Designated Providers(s), verification of these requests, running searches, managing search results, in terms of carrying out analyses and forwarding reports to those it considers relevant, etc. would all take place at central level. The key bodies involved in the system could be EUROPOL and Eurojust, or by EU bodies to be established. Member States, the US and, possibly, other third countries, would be recipients, without having an active role in the TFTS. Monitoring compliance with safeguards and controls would also be fully centralised, possibly involving oversight by external stakeholders.
B2. Decentralised system at MS level	**The national implementation of EU TFTS.** This policy option would involve the establishment of Member State TFTS units, by individual Member State (which would imply establishing a maximum of 27/28 national TFTS systems). The tasks and functions would thus be fully decentralised. This means that each Member State would be responsible for issuing requests for "raw" data to the Designated Provider(s) and for verifying these requests and that each will receive individual sets of data. The Member States would also be responsible for running searches and managing search results, in terms of carrying out analyses and forwarding reports to those it considers relevant. Monitoring compliance with safeguards and controls would also be fully de-centralised, possibly involving oversight by external stakeholders. The key bodies involved would be national law enforcement or intelligence authorities (separate bodies for issuing requests to Designated Provider(s) and for verifying these requests), with the possibility of creating new national bodies or introduce new units. Relevant data protection stakeholders would supervise processing activities and enforce compliance with data protection law.
B3. Hybrid systems	Several hybrid systems are possible, ranging from a very high to a very low level of EU involvement.

Policy Option	Description
B3.1 A central EU TFTS unit but MS are free to undertake their own searches.	**B3.1 The EU TFTS coordination and analytical service**. This policy option would involve an EU legislative instrument **establishing an EU central TFTS unit**, with most of the tasks and functions being implemented at the EU level. These would consist of issuing requests for "raw" data to the Designated Providers(s), verification of these requests, running searches, handling requests for searches and managing search results, in terms of carrying out analyses and forwarding reports to those who requested searches or to those it considers relevant, etc. Requests for "raw" data to be issued to the Designated Provider(s) would be prepared in consultation with the Member States. **Member States could opt to either request searches to be run on their behalf by the central unit (having to substantiate their requests for searches and the nexus to terrorism to the central unit), or undertake their own searches,** through designated national TFTS analysts which would be based in the same location as the EU TFTS unit. The extent to which such requests are substantiated and have a nexus to terrorism could be verified and validated at EU national level for searches by EUROPOL and at national level for Member State searches. Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders. Data protection, integrity and security would also be ensured at the central level. The key bodies involved in the system could be EUROPOL and Eurojust. Alternatively, the possibility of creating new bodies could be included, or the appointment of other existing ones. At national level, the key bodies involved would be national law enforcement and intelligence authorities, with the possibility of creating new national bodies. Relevant data protection stakeholders would supervise processing activities and enforce compliance with data protection law.
B3.2 An EU central unit which runs own as well as MS searches.	**B3.2 EU TFTS extraction service**. This policy option would involve an EU legislative instrument **establishing a EU central TFTP unit**, whose tasks would comprise issuing requests for "raw" data to the Designated Providers(s), verification of these requests, running searches, handling requests for searches and preparing search results in a presentable manner, without analysis. Requests for "raw" data to be issued to the Designated Provider(s) would be prepared in consultation with the Member States. **Member States would request searches to be run on their behalf.** The extent to which such requests are substantiated and have a nexus to terrorism would be verified and validated at national level. The EU central TFTP unit would run the search and return the full set of results, organised in a presentable manner, to the Member States. The EU central TFTP unit would be able to conduct searches and analyse the results on behalf of EU institutions, the US and, possibly, other third countries. It could also opt for spontaneous provision of information. Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders. Data protection, integrity and security would also be ensured at the central and national levels. The key bodies involved in the system could be EUROPOL and Eurojust. Alternatively, the possibility of creating new bodies could be included, or the appointment of other existing ones. Relevant data protection stakeholders would supervise processing activities and enforce compliance with data protection law.
B3.3 An ad-hoc EU level authority, probably by upgrading the current FIU Platform.	**B3.3 The FIU coordination service.** This policy option would involve the establishment of an EU legislative instrument **establishing an ad-hoc EU level authority,**

Policy Option	Description
	possibly by upgrading the FIU Platform, made up of all Member State FIUs. The tasks and functions would, in part be centralised and in part be decentralised. The upgraded FIU Platform would issue requests for "raw" data to the Designated Provider(s), by compiling the needs specified by the FIUs into a single request. The data could be centrally stored with the IT Agency, but made available (either physically or via secure connections) to the FIUs. Each FIU would be responsible for running searches and managing search results on behalf of their Member State, in terms of carrying out analyses and forwarding reports to those it considers relevant. The extent to which searches are substantiated and have a nexus to terrorism would be verified and validated at national level. Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders. Data protection, integrity and security would also be ensured at the central level. Relevant data protection stakeholders would supervise processing activities and enforce compliance with data protection law.
B4 Retention / Extraction As mentioned above, these two options have been included at the request of some Members of Parliament following the publication of the Commission's Communication on possible options in July 2011. These MEPs expressed the opinion that, personally, they had a mere retention/extraction system in mind when agreeing to the EU-US TFTP Agreement. As a consequence, the Commission decided to expand the assessment to include the analysis of these two additional options und B.4.	**B.4.1 Data retention regime**. Under this policy option, the Designated Providers would be required to retain the data on its server for a certain period (to be determined). The option would eliminate the need to make requests for "raw" data and the related verification process. The storage of the data would remain with the Designated Providers. Access to the retained data could either be granted to the US, possibly by amending the EU-US TFTP Agreement, or be expanded to other stakeholders, including EUROPOL (also for requests for searches from third countries) and Member State responsible authorities. The US and Member States would need to 'substantiate' each request and its nexus to terrorism before a search could be initiated with their respective national authorities. The Designated Provider would run the search and return the full set of search results to those requesting it. If technically feasible, it may be considered to encrypt both the searches and the search results. Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders.
	B.4.2 Data retention regime and extraction system. This option would be the same as the previous option. However, contrary to B.4.1, a search facility would be created on the premises of the Designated Provider(s) or in a facility very near to the latter (to allow for a direct, highly secured connection, with searches being directly carried out by a central unit consisting of analysts from the US and possibly from EUROPOL and Member States. Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders.

Options A.2 and A.3 as well as options B.1 and B.2 have been discarded mainly for reasons of legal and/or technical impracticability.

A.2: The fact that this option depends on the consent of a third country makes it weak. The policy option would also not have a guaranteed positive impact on ensuring the full protection of fundamental rights. In addition, this policy option is expected to have considerable implementation costs, arising from the relocation of the existing EUROPOL TFTP analysts to the US Treasury. Additionally, it is assumed that several Member States would also locate analysts in the US which would generate additional costs. Finally, several practical problems

are likely, related to the US potential reluctance to allow Member States full access to the system, besides possible legal implementation difficulties.

A.3: This option would considerably worsen the current situation. The US TFTP would continue to exist, but only data from the Transatlantic zone could be searched (and not intra-European zone data), which will make the system even less adapted to EU intelligence requirements in the EU. In addition, in the absence of the EU-US TFTP agreement, it may be unlikely that the US would accept requests for searches from the EU and Member States and /or provide leads spontaneously. Member States had no access to relevant data necessary for the prevention of terrorist offenses in the EU.

B.1: This option would also worsen the current situation as it could not effectively contribute to preventing terrorism and enhancing security. Even if a centralised system enhanced the technical capability at EU level, its application would still be limited in view of the imperfect inputs due to the lack of necessary intelligence and the absence of a connection with the Member States.

In addition, this policy option would involve a significant initial outlay for developing the physical and technical infrastructure of a centralised EU unit. It is assumed that the US will not share the software and technical know-how under this option. Initial set-up costs are estimated to be in the range of € 8 million to 10 million if a new, secure facility is to be created to 'house' the system. If existing facilities are upgraded to meet the enhanced security requirements, then the costs are estimated to be around € 3-3.5 million less but are still considerably high.

The practicability of the centralised system is rather low, primarily due to the anticipated limited utility of the system, in the absence of underlying intelligence. It would be indispensable to set up clear data protection, integrity and security arrangements, including the monitoring of compliance with safeguards and judicial protection of citizens.

The acceptance of the centralised system is low, as Member States did not consider it a viable option in the expert meetings and at Council Committees' discussions.

B.2: This option would clearly worsen the current situation. A decentralised system, operated by each national law enforcement authority in isolation, would only cater the intelligence requirements of individual Member States. Several may even not have the capacity to implement a national TFTS. Due to this deficiency, the overall objective of preventing terrorism could not be achieved as effectively as with the current system or other possible options.

In addition, there would be a very negative impact on the protection of fundamental rights of European citizens when processing financial messaging data. The policy option would mean that different sets of data are transferred to up to 27/28 Member States. Also, there is a great risk of links being missed and fragmentation of intelligence.

There would be an important impact on Member States' budgets as this policy option would involve a significant initial outlay for developing the physical and technical infrastructure for national TFTS, estimated to be in the range of € 101 million to 133 million. In addition, the annual running costs are expected to be in the range of € 62 million to 68 million. These costs

include the maintenance costs of the TFTS, staff costs, operational costs such as training, travel etc.

VI. ANALYSIS OF IMPACTS

The detailed analysis of impacts is limited to the short listed options, which include six options concerning the structure of the system in general: the status quo (A.1), three hybrid systems (B3.1-B.3.3) and two data retention systems (B.4.1.-B.4.2).

The criteria used for assessing the options have been effectiveness, impact, practicability and feasibility. Due to the fact that the specific policy objectives are to a certain extent correlated and mutually interdependent, an overall score is indicated for the effectiveness criterion.

Table 1.2 Overview of Assessment Criteria

Main Criterion	Parameters
Effectiveness	The extent to which the policy option will contribute to the achievement of: General policy objective • Preventing terrorism and enhancing security Specific policy objectives • Ensuring that the system is tailored to respond to EU's intelligence requirements given its threat assessment • Increasing the EU and Member State capability to analyse financial messaging data and to identify links between individuals/ groups involved in terrorism or its financing. • Maintaining effective cooperation with the US and other third countries in the fight against terrorism • Ensuring that the analysis of financial messaging data covers all relevant service providers and message types (the extent to which this specific objective is fulfilled depends on the implementation choices of the scope of an EU TFTS and it is therefore not considered in the assessment of the options but in the assessment of the implementation choices only*)* • Ensuring full protection of the rights of European citizens to privacy and data protection when accessing and analysing financial messaging data. Examination under this specific objective will explore whether the rights of European citizens to privacy and data protection are 'better' protected than in the current situation. It will be also be examined whether the right to private life and the protection of personal data can be subjected to the limitations and conditions defined in Article 8 of the European Convention of Human Rights and Article 52 of the Charter on Fundamental Rights of the European Union. These limitations permit interferences that are in so far as necessary "*in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*", "*in accordance with the law" and "necessary in a democratic society*". This will also entail considerations on the proportionality of the policy options. The assessment also includes considerations on the different 'stages' for which appropriate data protection measures will need to be put in place, namely (if applicable depending on the policy option) for the preparation of bulk data, its transport, the storage, the running of searches, the saving of search results and the dissemination of search results. Especially with regard to the latter, in a system which involves multiple Member States, it will also be important to consider whether different levels of Member State intelligence / law enforcement authorities are actually allowed to exchange information, even if they would be willing to do so. Issues such as access, rectification / erasure and redress should also be taken into account.
Impact[19]	**Economic impact** (see also Annex 2)**:** • Direct costs to EU and MS budgets of implementing and administering the policy option;

Table 1.2 Overview of Assessment Criteria	
Main Criterion	**Parameters**
	The calculation of the costs relies on information provided by the US on the establishment of their TFTP system at a meeting with the contractor for the Impact Assessment study. As the current US system is the only comparable mechanism in place, there was no other possibility to work with other actual figures in this context. The costs are further detailed in Annex 2. Administrative and compliance costs for affected businesses; As a result of the further research on the market of financial messaging services, it has become clear that, if other Designated Providers are included in an EU TFTS, the costs may vary per type of provider, also depending on how they currently store information on payments. • Indirect costs to the economy in general; • Wider economic impact resulting from reduced threat and incidence of terrorism **Social impact:** public perception of safety, security and equality The social impact relates to a large extent on difficult to prove perceptions related to a terrorist threat in public opinion. Evidence for such a perception is difficult to obtain. That is why the assessment of this criterion will need to rely on probability estimations. **Impact on fundamental rights**: assessed as part of the achievement/effectiveness **Political impact**: Likely impact on relations with the US and other third countries.
Practicability	**Risk assessment***:* can risks be identified and either mitigated or allocated and managed? **Affordability:** are sufficient budget funds available to implement the option? **Implementation capacity**: what about availability of technical expertise, physical resources e.g. buildings, offices etc., IT capacity? As part of this assessment, it will be important to look at the extent to which a maximum level of IT and physical security can be offered in order to ensure the protection of personal data. **Complementarity** with the US system: does the policy option allow for effective interface with the US-TFTP ensuring that intelligence does not fall through the cracks **Legislative issues:** to what extent new legislative instruments have to be introduced and/ or existing ones changed as a result of implementing a particular policy option?
Feasibility	**Political feasibility**; are policy and decision makers likely to sign up to a particular policy option and what would be the main hurdles in this respect? **Public acceptability**: would the option be acceptable to the general public? As for the reasons referred to above, no broad public consultation could be carried out, the analysis of this point will need to rely on the individual views by certain stakeholders and some citizens expressed after the publication as well as on assumptions based on comparable public input, such as that received in context of the entry into force of the EU US TFTP Agreement.

The economic impacts of the options have to rely on estimates and assumptions. Above all the possible economic benefits are not easy to measure, even though the European Commission is aware that in other contexts, such as in relation to health issues this might be undertaken by applying the "Quality adjusted life year" methodology. In the context of terrorism, however, it appears impossible and disproportionate to try to weigh by figures the value of human lives that could be saved by preventing terrorist attacks. It is also not possible to predict in detail the economic benefits of such a system helping to prevent terrorist activity and the damages it causes to the economy or state-owned or private property as the extent of attacks and the damages caused depend on a great number of unpredictable variables. Likewise, the social and psychological impact of terrorist attacks is difficult to quantify (e.g. the Madrid 2004 attacks had 1% casualties but a continental wide impact).

In addition, it needs to be recalled that the present mechanism is meant to be a security policy instrument. Data available in this context is highly confidential in order to prevent that those that shall be tackled by the instrument are not in a position to circumvent it or adapt their criminal and terrorist behaviour in a way that the system would not be able to detect them. This limits for this specific Impact Assessment the possibility to provide the same detail when identifying, assessing and comparing impacts as one may be used to from similar exercises in other policy fields. Finally, a great amount of information used for the analysis carried out stems from a third country source (US) that has practical experience with a similar system to fight terrorism and its financing. This information is to a large extent classified as it is essential for the security situation in this country (US). Even if it cannot be made public in this assessment, the European Commission was able to consider important parts of it in its analysis of the issue at stake.

Consequently, the indications below had to be based on certain assumptions which are laid down and further explained in Annex 1. Annex 2 includes a detailed list to explain the costs caused by the individual options.

The assessment criteria are, where feasible, accompanied by a 'rating', which 'scores' the policy options in relation to the status quo option, using the following scale:

-1 to -10	0	1 to 10
Costs/ worsening of situation compared to 'status-quo' -1 = little negative impact -10 = huge negative impact	**No change** from 'status-quo'	Benefits/ improvement compared to 'status-quo' 1= little positive impact 10= huge positive impact

The absolute value of 1 to 10 is not really important. The ratings of the options matter in relation to the status quo and to each other. The explanations for the ratings are elaborated in the respective assessment of each criterion.

Option A Status Quo (Continuation of EU-US TFTP Agreement)

Category of impact	Rating (-10 to +10)	Explanation
Achievement of objectives/ Effectiveness/ Fundamental Rights		
No change. The EU and the Member States will continue to be able to request searches to be run by the US and will receive leads provided spontaneously by the US. These will have some positive impact on the prevention of terrorism and enhancing security. The current system is not tailored to the EU's intelligence requirements and threat assessment, which may limit the searches which can be requested by the Member States (e.g. as certain countries or categories of messages may not be included). The current relations and coverage of Data Providers and message types would remain unaltered as well as the EU and Member States capabilities in this respect. However, the EU US Agreement on the TFTP, as confirmed by the two reviews, is not only a valuable instrument for effective cooperation between the two parties in fight against terrorism but it also has turned out to increasingly serve EU security needs by enhancing reciprocity. Fundamental rights: The situation as described in the Commission's report on the second joint review on the application of the EU US TFTP Agreement will be kept. The two reviews on the application of the Agreement by the Commission have verified that the comprehensive safeguards included in it, in particular those related to personal data protection, are properly implemented and that no major concerns exist. There would be no additional data collection mechanism which could infringe personal data protection rules.		

Category of impact	Rating (-10 to +10)	Explanation
	0	
Economic impact		
Direct financial cost - implementation costs	0	No change.
Benefits	0	No change.
Other impact		
Social impact	0	No change.
Political impact	0	No change.
Other issues		
Practicability	0	Some improvement in the longer term may occur, as for example Member States will make more use of the possibility to request searches to be run
Feasibility	0	No change

Category of impact	Rating (-10 to +10)	Explanation
Achievement of objectives/ Effectiveness/ Fundamental rights		
Overall positive impact on the extent to which the policy option can contribute to the prevention of terrorism and enhancing security. A hybrid system managed by EUROPOL but with national inputs in terms of running searches and analysing their results would ensure that the specific intelligence requirements of the EU and Member States are fully taken into account and that the system is geared towards the specific "EU threat". It can be expected that, in the medium term, a joint TFTS, i.e. with EUROPOL and Member States working alongside each other, would lead to increased trust and synergies, thus overcoming scepticism and boosting the EU cooperation in the fight against terrorism. The policy option would increase the capacity of the EU and Member States to independently search and analyse financial messaging data and to identify and map links. Fundamental rights: The limitation of the rights to privacy and data protection, through application of Article 52, could arguably be regarded as proportional, i.e. necessary and appropriate for the purpose of combating terrorism over other less intrusive alternatives, considering additional security gains expected from the system. In any case robust data protection guarantees and safeguards will have to be put in place as the system implies an interference with private life and the protection of personal data.	**0**	
Economic impact		
Direct financial cost - implementation costs (see also Annex 2)	**-3**	Impact on EU Budget: Initial set-up costs are estimated to be in the range of € 5.3 million to 6.5 million if new, secure facilities are to be created to 'house' the systems. If existing facilities are upgraded to meet the enhanced security requirements, then the costs are estimated to be reduced by around € 3-3.5 million Impact on Member State Budget: This policy option would involve a small initial outlay on part of Member States (€ 354,000 to 503,000) as they would need to develop protocols for liaising with the central EU unit; 14member States would be relocating TFTS analysts to the centralised EU agency The Designated Provider will have to invest in the range of € 455,800 to 708,000. Impact on EU Budget: running costs are expected to be in the order of € 6.3-6.7 million Impact on Member State Budget: the annual running costs are expected to be in the order to € 2 million. These costs include staff costs and operational costs such as training, travel etc. Impact on Designated Provider: the annual running costs are expected to be in the order of e 0.7 million, stemming from the salary and operational costs. Administrative costs are estimated to be in the range of € 46,190 to 79,060 for the EU, € 70,280 for the Member States and € 15,354 for the Designated Provider.
Benefits	**+3**	The policy option is expected to reduce the level of minor terrorist activity and the likelihood of a major terrorist attack This would result in the prevention of deaths and casualties as well as financial losses caused by the attacks themselves and subsequent consequences.
Other impact		
Social impact	**0**	It is likely that some positive impact would occur, as public perception of safety and security should improve if, like it is the case in the second joint review report on the EU US TFTP Agreement, actual cases in which the system helped to prevent terrorist acts, are presented to the public by a report. However, as letters to the European Commission at the time of the entry into force of the EU US TFTP Agreement have shown, citizens are very sensitive regarding increased data control by authorities which could outweigh the positive social impact.
Political impact	**0**	Neutral impact. There have been no indications from US side that such a system would be regarded as detrimental to their interests.
Other issues		
Practicability	**+1**	The overall practicability of the policy option is reasonable, primarily because it would combine EU and national search capacities in a single

Category of impact	Rating (-10 to +10)	Explanation
		system. In the medium term and provided information is increasingly shared, it is expected to boost the overall analytical capacity of the EU. The option would allow for effective interface with the US system, provided it is built on the same parameters. It would be paramount to set up clear data protection, integrity and security arrangements, including the monitoring of compliance with safeguards and judicial protection of citizens.
Feasibility	**-1**	Given their potential involvement in the "core" of this TFTS, Member States may overall consider this policy option politically viable. There might be some resistance regarding additional expenses due to the financial budgetary constraints caused by the current economic crisis.

Option B.3.2 Hybrid system - The EU TFTS Extraction Service

Category of impact	Rating (-10 to +10)	Explanation
Achievement of objectives/ Effectiveness/ Fundamental rights		
Overall some positive impact on the extent to which the policy option can contribute to the prevention of terrorism and enhancing security. A hybrid system in which Europol would run searches on behalf of national law enforcement agencies and only delivers search results would primarily be responsive to the specific intelligence requirements of the individual Member States. By attributing a "bureau" function to EUROPOL and not allowing it to undertake analysis of national searches, the benefits of EU level analysis would not occur and there is a risk of links being missed and fragmentation of intelligence. Fundamental rights: The limitation of the rights to privacy and data protection, through application of Article 52, could arguably be regarded proportional, i.e. necessary and appropriate for the purpose of combating terrorism over other less intrusive alternatives, considering the positive security gains expected. In any case robust data protection guarantees and safeguards will have to be put in place as the system implies an interference with private life and the protection of personal data. Due to the system's architecture, there would be a high risk that the searches are insufficiently narrowed down and will thus contain many "false positives", i.e. details on innocent persons, which are subsequently forwarded to the Member States without any further central control of their use.	**0**	
Economic impact		
Direct financial cost - implementation costs (see also Annex 2)	**-3**	Impact on EU Budget: Initial set-up costs are estimated to be in the range of € 5.3 million to 6.5 million if new, secure facilities are to be created to 'house' the systems. If existing facilities are upgraded to meet the enhanced security requirements, then the costs are estimated to be reduced by around € 3-3.5 million Impact on Member State Budget: This policy option would involve a small initial outlay on part of Member States (€ 354,000 to 503,000) as they would need to develop protocols for liaising with the central EU unit. The Designated Provider will have to invest in the range of € 455,800 to 708,000. Impact on EU Budget: running costs are expected to be in the order of € 4.9-5.3 million Impact on Member State Budget: the annual running costs are expected to be in the order to € 10 million. These costs include staff costs and operational costs such as analytical capacity, control and oversight, training, travel etc. Impact on Designated Provider: the annual running costs are expected to be in the order of € 0.7 million, stemming from the salary and operational costs. Administrative costs are estimated to be in the range of € 46,190 to 79,060 for the EU, € 70,280 for the Member States and e 15,354 for the Designated Provider.
Benefits	**+2**	The policy option is expected to reduce the level of minor terrorist activity and the likelihood of a major terrorist attack. This would result in the prevention of deaths and casualties as well as financial losses caused by the attacks themselves and subsequent consequences. However, by attributing a "bureau" function to EUROPOL and not allowing it to undertake analysis of national searches, the benefits of EU level analysis would not occur and there is a risk of links being missed and fragmentation of intelligence. , there is a

Category of impact	Rating (-10 to +10)	Explanation
		very high risk that the searches are insufficiently narrowed down and will thus contain many "false positives", i.e. details on innocent persons, which are subsequently forwarded to the Member States without any further central control of their use.
Other impact		
Social impact	0	It is likely that some positive impact would occur, as public perception of safety and security may improve if, like it is the case in the second joint review report on the EU US TFTP Agreement, actual cases in which the system helped to prevent terrorist acts, are presented to the public by a report. The TFTS shows its effectiveness (and if this is communicated to the public). However, as letters to the European Commission at the time of the entry into force of the EU US TFTP Agreement have shown, citizens are very sensitive regarding increased data control by authorities which could outweigh the positive social impact.
Political impact	0	Neutral impact. As above.
Other issues		
Practicability	-1	The overall practicability of the policy option is rather low, primarily because it would combine EU searches with national analytical capacity in a single system, reducing the extent to which synergies can be created and a full "EU picture" generated. It would be paramount to set up clear data protection, integrity and security arrangements, including the monitoring of compliance with safeguards and judicial protection of citizens.
Feasibility	-1	It is likely that a fair share of Member States, especially those with well-developed law enforcement bodies dealing with counter-terrorism and those being sceptical about EUROPOL capacity to provide effective analyses of search results, will consider this policy option acceptable. Other Member States, however, with less capacities and/or a better opinion on EUROPOL analysis abilities find this option less acceptable. There might be some resistance regarding additional expenses due to the financial budgetary constraints caused by the current economic crisis.

Option B.3.3 Hybrid system - The FIU coordination service

Category of impact	Rating (-10 to +10)	Explanation
Achievement of objectives/ Effectiveness/ Fundamental rights		
Overall some positive impact on the extent to which the policy option can contribute to the prevention of terrorism and enhancing security. The existing level of connectivity between the FIUs would, to some extent, limit the risk of links being missed and fragmentation of intelligence. Search results would primarily be responsive to the specific intelligence requirements of the individual Member States. Furthermore there is a risk that the system will separate financial intelligence from other intelligence and this separation could constitute a major drawback and a narrowness of vision. It would primarily enhance capabilities at national level, with FIUs already having substantial expertise in the area of terrorism financing. The policy option would provide the US and third countries with a single point of contact. Fundamental rights: The extent to which the limitation of the rights to privacy and data protection, through application of Article 52, would be proportional, i.e. necessary and appropriate for the purpose of combating terrorism over other less intrusive alternatives, is questionable. Whilst security gains are likely to occur, these may not outweigh the disadvantages of the system's decentralised architecture. In any case robust data protection guarantees and safeguards will have to be put in place as the system implies an interference with private life and the protection of personal data.	0	
Economic impact		
Direct financial cost - implementation costs (see also Annex 2)	-3	Impact on EU Budget: Initial set-up costs are estimated to be in the range of € 5.5 million to 6.8 million if new, secure facilities are to be created to 'house' the systems. If existing facilities are upgraded to meet the enhanced security requirements, then the costs are estimated to be reduced by around € 3-3.5 million Impact on Member State Budget: This policy option would involve a small

Category of impact	Rating (-10 to +10)	Explanation
		initial outlay on part of Member States (€ 354,000 to 503,000) as they would need to develop protocols for liaising with the central EU unit; 14member States would be relocating TFTS analysts to the centralised EU agency The Designated Provider will have to invest in the range of € 455,800 to 708,000. Impact on EU Budget: running costs are expected to be in the order of € 5.6-6 million Impact on Member State Budget: the annual running costs are expected to be in the order to € 22 million. Member States would need to train and deploy TFTS analysts and also enhance their oversight, control and data protection capacity. Impact on Designated Provider: the annual running costs are expected to be in the order of € 0.7 million, stemming from the salary and operational costs. Administrative costs are estimated to be in the range of € 46,190 to 79,060 for the EU, € 70,280 for the Member States and € 15,354 for the Designated Provider.
Benefits	+2	The policy option is expected to reduce the level of minor terrorist activity and the likelihood of a major terrorist attack. This would result in the prevention of deaths and casualties as well as financial losses caused by the attacks themselves and subsequent consequences. However, given the risk that the system will separate financial intelligence from other intelligence and that this separation could constitute a major drawback and a narrowness of vision, the possible benefits could be reduced.
Other impact		
Social impact	0	Neutral effect. Public perception of safety and security will improve if the TFTS shows its effectiveness (and if this is communicated to the public). This may be limited by the fact that overall awareness of FIUs is low. In addition, as here are several authorities involved (all EU FIUs), it is likely that EU citizens would consider that they were being 'watched' by a multiplicity of national FIUs.
Political impact	0	Neutral impact. As above.
Other issues		
Practicability	-1	The overall practicability of the policy option is limited, considering the lack of a clear EU involvement, a potentially too narrow focus and the substantial efforts required for its set up. Also, the extent to which national FIUs are well developed and have the legal standing and capacity to undertake the tasks required will vary. It would be paramount to set up clear data protection, integrity and security arrangements, including the monitoring of compliance with safeguards and judicial protection of citizens.
Feasibility	0	The extent to which Member States will consider the policy option acceptable will vary greatly, with some (including the initial proposing country) being very much in favour and others very much against. At the level of the EU, there will be concerns about the creation of a new EU body. There might be some resistance regarding additional expenses due to the financial budgetary constraints caused by the current economic crisis.

Option B.4.1 Data retention / extraction – Data retention regime

Category of impact	Rating (-10 to +10)	Explanation
Achievement of objectives/ Effectiveness/ Fundamental rights		
Small positive impact on the extent to which the policy option can contribute to the prevention of terrorism and enhancing security, provided that access to the data retained is also granted to Europol and/or Member States. There is a risk of links being missed and fragmentation of evidence in the absence of some form of coordination at		

Category of impact	Rating (-10 to +10)	Explanation
EU level of the searches and the use of search results which would primarily be responsive to the specific intelligence requirements of the individual Member States. Fundamental rights: The extent to which the limitation of the rights to privacy and data protection, through application of Article 52, would be proportional, i.e. necessary and appropriate for the purpose of combating terrorism over other less intrusive alternatives, strongly depends on whether Europol and the Member States would also have access to the system. As non-analysts would run searches, there is a great risk of 'false positives' , i.e. details on innocent persons, which are subsequently forwarded to the Member States. Furthermore each Member State would be initiating its own search hence no uniform approach would be ensured in accessing the personal data and their handling. Entrusting the designated provider with running the searches would further increase the risk of infringements of data protection requirements. In any case robust data protection guarantees and safeguards would have to be put in place as the system implies an interference with private life and the protection of personal data.	**-1**	
Economic impact		
Direct financial cost - implementation costs (see also Annex 2)	**-2**	Under this option the EU would develop and install the TFTS on the Designated Provider's premises. At EU level, a system and protocol would need to be developed, for liaising with the Designated Provider to request searches and to obtain search results. These are estimated to amount to around € 0.7 and 1.2 million. Member States would contribute to the development of protocols in relation to liaison with the Designated Provider. These would entail a relatively small cost (€ 284,000 to 433,000). The Designated Provider would also have to adapt internal systems and procedures to meet the requirements of the EU TFTS; obtain security clearance for staff involved in TFTS and provide them with initial training. The costs of the above activities are expected to be in the range of € 759,800 to € 913,000. Impact on EU Budget: running costs are expected to be in the order of € 1.8 million Impact on Member State Budget: the annual running costs are expected to be in the order to € 1.7 million. These costs include staff costs and operational costs such as training, travel etc. Impact on Designated Provider: the annual running costs are expected to be in the order of € 1.6 million, stemming from the salary and operational costs of 11 FTE posts Administrative costs are estimated to be in the range of € 46,190 to EUR 79,060 for the EU, € 70,280 for the Member States and € 15,354 for the Designated Provider.
Benefits	**+1**	The policy option is expected to reduce the level of minor terrorist activity and the likelihood of a major terrorist attack. This would result in the prevention of deaths and casualties as well as financial losses caused by the attacks themselves and subsequent consequences. However, given the risk of fragmentation of evidence in the absence of some form of coordination at EU level of the searches and the use of search results the extent of the benefits should be rather limited. This is also due to the element that non-analysts would run searches which creates a greater risk of 'false positives'.
Other impact		
Social impact	**0**	Some positive impact would occur, as public perception of safety and security may improve if the TFTS shows its effectiveness and if concrete case examples can be demonstrated as it is the case in the report on the second joint review of the EU US TFTP Agreement. However, based on some citizen letters received by the Commission in the context of the entry into force of that Agreement, the fact that this system would constitute an additional basis for the retention of personal data that public authorities would have access to this data on the premises of the Designated Providers is very likely to neutralise the positive impact.
Political impact	**-4**	Negative impact. The US would consider that this model would not be effective compared to the current practice.
Other issues		
Practicability	**-4**	The overall practicability of the policy option is rather low in general, due to the reduced possibility to create synergies and a full "EU picture". This is

Category of impact	Rating (-10 to +10)	Explanation
		further worsened various legal and technical reasons. Applying a data retention regime on Designated Providers could require disproportionate efforts. For example, for the current Designated Provider, a requirement to extract data on transactions of *individual* persons and organisations (i.e. single account holders) would change the business model of the latter entirely. Legally, it would also be complex to create an instrument which would require data retention by Designated Providers, possibly for the sole purpose of extracting data requested by a third country (i.e. the US). Finally, it would be paramount to set up clear data protection, integrity and security arrangements.
Feasibility	**0**	The policy option would address some of the concerns raised in the European Parliament, who had called for an extraction system only. Member States, however, were less supportive.

Option B.4.2 Data retention / extraction – Data retention regime and extraction system

Category of impact	Rating (-10 to +10)	Explanation
Achievement of objectives/ Effectiveness/ Fundamental rights		
Small positive impact on the extent to which the policy option can contribute to the prevention of terrorism and enhancing security, provided that access to the data retained is also granted to Europol and/or Member States. There is a risk of links being missed and fragmentation of evidence in the absence of some form of coordination at EU level of the searches and the use of search results which would primarily be responsive to the specific intelligence requirements of the individual Member States. Fundamental rights: The extent to which the limitation of the rights to privacy and data protection, through application of Article 52, would be proportional, i.e. necessary and appropriate for the purpose of combating terrorism over other less intrusive alternatives, strongly depends on whether Europol and the Member States would also have access to the system. As non-analysts would run searches, there is a great risk of 'false positives', i.e. details on innocent persons, which are subsequently forwarded to the Member States. Furthermore each Member State would be initiating its own search hence no uniform approach would be ensured in accessing the data and their handling. Entrusting the designated provider with running the searches would further increase the risk of infringements of data protection requirements. In any case robust data protection guarantees and safeguards will have to be put in place as the system implies an interference with private life and the protection of personal data.	**-1**	
Economic impact		
Direct financial cost - implementation costs (see also Annex 2)	**-3**	Under this option the EU would develop and install the TFTS on the Designated Provider's premises. TFTS analysts would be located on Designated Provider's premises (both, EU and national analysts) Initial EU set-up costs are estimated to be in the range of € 2.2 million to 2.9 million. Member States would contribute to the development of protocols in relation to liaison with the Designated Provider and would incur relocation cost of national analyst (€ 354,000 - €503,000). The Designated Provider(s) would also have to adapt internal systems and procedures to meet the requirements of the EU TFTS; obtain security clearance for staff involved in TFTS and provide them with initial training. The costs of the above activities are expected to be in the range of € 755,000 to € 907,000. Impact on EU Budget: running costs are expected to be in the order of € 4.7 -5.1 million The annual running costs for Member States are expected to be in the order to € 2 million. These costs include staff costs and operational costs such as training, travel etc. Impact on Designated Provider: the annual running costs are expected to be in the order of EUR 0.7 million, stemming from salary and operational costs. Administrative costs are estimated to be in the range of € 46,190 to € 79,060 for the EU, € 70,280 for the Member States and € 15,354 for the Designated Provider.

Category of impact	Rating (-10 to +10)	Explanation
Benefits	+2	The policy option is expected to reduce the level of minor terrorist activity and the likelihood of a major terrorist attack to a greater extent than the previous due to the actual presence of Europol and Member States' experts at the Designated Provider's premises. Important would be that access to the data is provided to Member States and Europol. This would result in the prevention of deaths and casualties as well as financial losses caused by the attacks themselves and subsequent consequences.
Other impact		
Social impact	0	Some positive impact would occur, as public perception of safety and security may improve if the TFTS shows its effectiveness as referred to above. However, the fact that this system would constitute an additional basis for the retention of personal data that public authorities would have access to this data on the premises of the Designated Providers would neutralise the positive impact.
Political impact	-4	Negative impact. The US considers that this model would not be effective compared to the current practice.
Other issues		
Practicability	-4	The overall practicability of the policy option is rather low in general, due to the reduced possibility to create synergies and a full "EU picture". This is further worsened various legal and technical reasons. Applying a data retention regime on Designated Providers could require disproportionate efforts. For example, for the current Designated Provider, a requirement to extract data on transactions of *individual* persons and organisations (i.e. single account holders) would change the business model of the latter entirely. Legally, it would also be complex to create an instrument which would require data retention by Designated Providers, possibly for the sole purpose of extracting data requested by a third country (i.e. the US). Finally, it would be paramount to set up clear data protection, integrity and security arrangements.
Feasibility	0	The policy option would address some of the concerns raised in the European Parliament, who had called for an extraction system only. Member States, however, did not express explicit support for this option in the meetings where this was discussed.

All options and sub-options above are regarded as possible implementing choices and are considered for comparison in this impact assessment. For practical reasons and as regards the scope of a possible new system the analysis of the implementing choices and their comparison with regard to the possible new system will only be carried out after having chosen a preferred implementing choice.

VII. COMPARING THE OPTIONS

VII.1 The structure of a new system

Each system has advantages and disadvantages, but based on the analysis detailed above, the hybrid policy options receive the highest scores. Of these, the EU TFTS coordination and analytical service (B3.1) is considered to be able to contribute most to the achievement of the policy objectives. In particular, due to its 'shared approach' it is expected to be most successful in increasing the EU and Member State capability to analyse financial messaging data and to identify links between individuals/ groups involved in terrorism or its financing.

This needs to be weighed against potential benefits and developments in the baseline scenario. At a dedicated meeting at EUROPOL in September 2012 and at a meeting hosted by the

European Commission in November 2012, Member States reported that they make more and more use of the "reciprocity" Articles 9 and 10 of the EU-US TFTP Agreement which shows that that system is transforming gradually into a reciprocal one. It provides Member States with information that they did not have at their disposal or did not benefit from at the time when the system was introduced. The reason for this is that they had not been sufficiently aware of this right. An awareness raising campaign by Europol as well as visits to Member States' capitals for information purposes carried out by Europol representatives has changed the practice and perception of the EU US TFTP agreement in Member States.

In addition, compared to option B.3.1 the baseline scenario reveals a number of further advantages. Contrary to option B.3.1 it does not lead to the accumulation of additional data and meets therefore no additional concerns with regard to an impairment of fundamental rights, in particular personal data protection provisions.

On one side the baseline scenario shows that the evolution goes towards meeting in an increasingly effective way the policy objectives of a possible EU TFTS, on the other it does not raise additional concerns with regard to an impairment of fundamental rights, in particular personal data protection provisions. Under these circumstances it becomes increasingly difficult to justify the necessity and proportionality of an additional system at present. In contrast to the situation at the time of the Council's call to the Commission in July 2010[20] or even at the time of the publication of the Commission's Communication in July 2011, Member States now take increasingly advantage of the data provided in the context of the TFTP. While concrete Member States' requests cannot be revealed in this context for confidentiality reasons, the latest Council discussions have clearly demonstrated a decreasing interest of Member States in establishing an additional EU system.

Furthermore, option B.3.1 would lead – like all options related to a new system – to considerable additional costs:

The initial set-up costs for option B.3.1 are estimated to be in the range of € 5.3 million to € 6.5 million if new, secure facilities are to be created to 'house' the systems. If existing facilities are upgraded to meet the enhanced security requirements, then the costs are estimated to be reduced by around 3-3.5 million but still could amount to € 3 million.

As also shown in part VI above, there would also be a direct impact on at least a number of Member States' budgets estimated between € 354.000 and 503.000 as they would need to develop protocols for liaising with the central EU unit.

As regards the costs for the Designated Providers, estimations of the investments needed are of € 455.800 to € 708.000 per Provider, to which running and further administrative costs would have to be added.

Last but not least, the impact on the EU Budget regarding the running costs is expected to be in the order of € 6.3-6.7 million and on the EU Member States' budgets of annually € 2 million.

These disadvantages show that maintaining the baseline scenario needs to be a serious option as well.

[20] Council Decision of 13 July 2010, OJ L 195, 27.7.2010, p.3

VII.2 Implementing choices for a new system

A) Choices for the purpose of an EU TFTS	
1 Combating terrorism	Access for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. This requires evidence of a proven nexus.
2 Combating terrorism and serious organised crime	Access for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing and for the purpose of other serious crimes.
B) Choices for the scope of an EU TFTS	
1 One Designated Provider	The system would only work with a single Designated Provider and hence exclusively access, search and analyse FIN messages.
2 Multiple Designated Providers	The system would work with multiple Designated Providers and hence access, search and analyse FIN and other types of financial messages / other types of data, potentially "suitable" categories or systems could include the Automated Clearing Houses, selected e-money services and selected remittance services.

VII.2.1 The purpose of a new system

As mentioned before, during the preparation of the Impact Assessment and due to the linkage between money laundering and terrorist financing in existing legislation, a number of Member States expressed the wish that the Commission should also look at the possibility of using a new EU TFTS also for the purpose of fighting organised crime.

In principle two possible approaches could be contemplated:

- the current approach under the TFTP, based on an access to the system for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. This requires evidence of a proven nexus.

- a broader approach, allowing access to the system for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing and for the purpose of other serious crimes

Expanding the purpose of a new system by including the fight against serious organised crime would undeniably enable law enforcement authorities to obtain additional financial data which could help in their fight against organised crime. However, overall, the widening of a new system's purpose would have overriding negative effects. In particular, it would raise concerns over its proportionality in view of its impact on the fundamental rights of those whose data would be affected.

With regard to human rights the impact would be very negative, primarily due to the disproportionally large volumes of the sets of bulk data which would be obtained from the Designed Provider(s), which can be accessed and searched without requiring the same level of justification as when limited to terrorism as the term of "serious crime" is much broader. Data would be processed for all serious crimes with a potential risk of uncertainties and diverging interpretations as to what is to be regarded as "serious" unless very rigid criteria, difficult to define, are agreed on what constitutes a nexus to serious crime. This means that the limitations to the rights to privacy and data protection implied by this option, although in

principle possible pursuant to Article 52 of the Charter, runs a high risk of being not proportional, i.e. necessary and appropriate for the purpose of combating terrorism compared to other less intrusive alternatives.

Another consequence of broadening the access would be that the US and EU systems would be different and not complementary. The US has limited the purpose of its TFTP to terrorism and terrorism financing only. Broadening the scope on the part of the EU might have a positive side effect for the US as they could benefit from the larger sets of bulk data that would be stored on the EU TFTS. However, this would create a lack of reciprocity and an imbalance to the mutual availability of data. In addition, third countries would be concerned about the fact that even more data on their citizen may be included.

In addition, the broad approach would inevitably lead to a substantial increase in costs. The implementing and running cost would rise as a higher number of analysts would be required to run all the additional searches for serious organised crimes and analyse the corresponding results; and higher volumes of data would need to be handled. However, the exact increase is difficult to estimate as there is no experience for such kind of system.

This choice would also likely have a negative social and political impact. Even if the general public perception of security and safety may increase, citizens have become sensitive when it comes to collecting personal data, in particular regarding their financial activities. The public perception that citizens and their activities are increasingly controlled by State entities might rise. The negotiations of the EU-US TFTP agreement have shown the extreme sensitivity around the use of privately-held or privately-collected personal data for law enforcement purposes which was reflected in discussions at the European Parliament and led to a disapproval of the first draft agreement by this institution. Therefore, expanding the system to cover all serious crimes would require clear definitions and very rigid criteria as to when a search can be run which can cause difficulties regarding their implementation, in particular in the hybrid models of the policy options B. This is putting into question the overall feasibility of such a system.

One can finally emphasise that, due to the very important negative effects on the protection of fundamental rights, political support by Member States and European Parliament has proven to be very low for a broad approach encompassing organised crime related data. Whilst some Member States considered the expansion of the purpose of the TFTS, theoretically, beneficial, none considered its expansion to all serious crimes acceptable or desirable.

VII.2.2 The scope of a new system

On the basis of the analysis of above referred payment categories, depending on the implementing choice, the scale of global and EU transactions covered for the monitoring and tracking of terrorists and those financing terrorism would vary. However, it will be key that the implementing measure chosen ensure that individual transactions are monitored and tracked in the most efficient way, thus ensuring the widest coverage of transactions with the lowest number of potential additional Designated Providers. When taking into consideration criteria such as size, relevance, adequateness, market concentration and FIN duplication, other players, such as Automated Clearing Houses, e-money and Remittance services could also be

valid and feasible sources of information for the monitoring and tracking of financial movements.

With regard to the scope of the system, including more than just FIN messages used by the current Designated Provider (option B) 2 – Multiple Designated Providers) would present clear advantages.

The analysis showed that FIN messages represent around 1% of the total payments market, which corresponds to nearly all (international) cross-border transfers. This means that domestic and intra-EU payments, as well as e-money transfers and remittances are not covered by the current system, whilst they could certainly be of great added value in identifying and mapping terrorist suspects and their financial movements.

If an EU system is to be better adapted to the specific EU interests, then it would be useful to also have access to transaction data to track financial movements within the EU via the above mentioned other providers.

It would also be important to ensure that the system would be 'future proof', by taking account of fast-growing new players, especially in the e-money services.

However, a proliferation of transaction data and related Designated Providers, within an EU context, faces major concerns regarding the proportionality of such a broadened scope. There will be significant impact on privacy and data protection rights. Therefore the potential addition of Designated Providers would need to be accompanied by rigid conditions, safeguards and control measures, to ensure appropriate data protection and oversight.

The much larger overall dataset to search would also inevitably lead to the necessity for the EU and the Member States to invest considerably in additional human resources and technical equipment for the collection and analyses of these data. The newly Designated Providers would also need to invest in setting up systems like the one the current Designated Provider has in order to comply with their new obligations. However, the exact and overall increase in costs is difficult to prove by concrete figures as there is no experience with such kind of system.

VII.3 Elaboration of the Preferred Option, incl. implementing choices

If an EU TFTS system was to be established, the comparison of those options single out policy option B.3.1 dedicated to the fight against terrorism funding and with a scope including Multiple Designated Providers. The system would thus be a hybrid system, which would make use of data from different money transfer services, including those linked to traditional banking, remittances and e-money.

However, as demonstrated above, it appears difficult to justify the EU added value of the introduction of a new and broader system. Potential impacts in terms of fundamental rights and substantial additional costs raise serious doubts with regard to the cost effectiveness of the establishment of a new system at this point of time compared to the existing possibilities of the TFTP and its positively assessed implementation.

Consequently, maintaining the baseline scenario and not presenting a legislative proposal for the introduction of an EU TFTS is the preferred option at this stage.

VIII. MONITORING AND EVALUATION

In close co-operation with Member States, the Commission will closely monitor the practical application of the EU US TFTP Agreement and the use of its reciprocity clauses by Member States and its practical impact and benefit for Member States' work on fighting terrorism and its financing. The Commission is actively involved in evaluating on an annual basis the application of the EU US TFTP Agreement in close-co-operation with relevant national data protection authorities, EUROPOL and the US. In addition, the Commission is in close contact with EUROPOL's Joint Supervisory Body (JSB) and carefully analyses the JSB's report on EUROPOL's work, including in the context of the application of the EU-US TFTP Agreement. All this will support the Commission in monitoring whether there are changes to the status quo which would provide new and relevant arguments for proposing the establishment of a new EU TFTS system based on the preferred options identified in this Impact Assessment.

The Commission intends to report back to the European Parliament and the Council on new developments and corresponding evaluations one year after the publication of this Impact Assessment.

IX. Annexes

IX.1 Annex 1 Overview of Specific Assumptions

For each policy options certain specific assumptions have been made regarding the costs and benefits. These are set out below.

Table 1.1 Specific Assumptions underpinning the Calculations for Different Policy Options

Policy Option	Costs	Benefits
A.1 – Status quo or Baseline	Cost to EU budget ▪ Verification and authorisation of US requests by Europol: 3 FTE X 2 days per month ▪ Initiating/ coordinating requests for spontaneous provision of information: 3 FTE X 1 day per month ▪ Independent EU overseer ▪ Independent review of the EU-TFTP Agreement ▪ Monitoring and reporting by the Commission The following running costs and administrative costs would accrue to the DP: ▪ Salary costs of 3 FTE overseers, 0.25 FTE involved in preparing and transmitting data, 0.25 FTE involved in provision of legal advice and guidance, 0.25 FTE involved in conducting external audit ▪ Updating the software and hardware ▪ Staff training – 5 to 6 days per staff per year ▪ Management time – 1 day of management time per month ▪ Staff time devoted to record keeping and reporting (2 FTE X 2 days per month) ▪ The assessment of costs accruing to DP are informed by interviews with DP	▪ Number of successful minor terrorist attacks per year = 94 ▪ Number of lives lost per year in minor terrorist attacks = 40 ▪ Number of persons injured in a minor terrorist attack = 359 ▪ Cost to Economy of a minor attack = € 162,896 ▪ Likelihood of a major terrorist attack = 90% ▪ Loss of Lives in a major attack = 100 ▪ Number of persons injured in a major terrorist attack = 500 ▪ Economic impact of a major attack = € 500 million to € 1 billion
A.2 – Status quo+ or Baseline	Initial set up costs: ▪ Development of EU legislative instrument (EU budget) ▪ Relocation of 4 existing Europol analysts to UST (EU budget) ▪ Relocation of 14 Member State analysts to UST (national budgets) – based on stakeholder consultations, it is clear that not all EU Member States face the same level of risk of terrorism. Member States that face a low risk of terrorism would not choose to relocate analysts at UST. Besides, there is likely to be a capacity constraint in terms of the number of EU analysts that can be accommodated at the UST ▪ Initial staff training (national budgets) Running costs ▪ Salary costs of analysts (EU + national budget) ▪ Operational expenditure of analysts (national	▪ Reduction in scale of minor terrorist activity = 0% ▪ Reduction in likelihood of a major terrorist attack = 10%

Policy Option	Costs	Benefits
	budget) ▪ Cost of independent overseer appointed by the EU (EU budget) ▪ Cost of issuing regular updates and guidance to intelligence staff (national budget) Administrative costs: ▪ Cost of monitoring and reporting by the Commission to the Council and the Parliament (EU budget) Cost to DP: Same as above (Option A.1)	
A.3 – Terminate EU-US TFTP Agreement	Not applicable	Increase in terrorist activity
B.1 – Centralised EU TFTS	The cost of setting-up and running the EU TFTS accrue to the EU budget. NB: The costs have been estimated on a conservative basis – actual costs might be lower depending on the extent to which existing Europol infrastructure and hardware could be used for the TFTS e.g. the costs include T1 lines. These might not accrue if Europol's Siena lines are deemed fit for purpose for the TFTS. Cost to DP: ▪ Same as Option A.1. Additionally, there would be one-off expenditure associated with ▪ Familiarisation with EU legislative framework and technical requirements ▪ Adapting existing systems and processes to comply with EU requirements ▪ Developing a data extraction system ▪ Initial staff training ▪ Security clearance of staff	▪ Reduction in scale of minor terrorist activity = 0% ▪ Reduction in likelihood of a major terrorist attack = 0%
B.2 – Decentralised System	Cost to EU budget ▪ The cost to EU budget would be those associated with the development of an EU legislative instrument Cost to national budgets ▪ The cost of developing and running the system would accrue national budgets. For reasons described earlier, it is assumed that 14 out of 27 Member States will choose to set up a national TFTS Cost to DP: ▪ the DP would have to incur an additional expenditure to familiarise with the EU/national legislation and systems (€75,000 to €100,000 X 14) ▪ It would cost the DP €200,000 to €400,000 to adapt/ set-up systems and processes to comply with the new requirements The following costs would be the same as B.1: ▪ Developing a data extraction system ▪ Initial staff training ▪ Security clearance of staff ▪ Running and administrative costs	▪ Reduction in scale of minor terrorist activity = 0% ▪ Reduction in likelihood of a major terrorist attack = 10%
B.3.1 - EU TFTS coordination and analytical service	Costs are same as B.1 except that (a) Member States can now request the central EU Agency to conduct searches on their behalf Member States could opt to either request searches to be run on their behalf by the central unit (having to substantiate their requests for searches or undertake their own searches, through designated national TFTS analysts which would be based in the same location as the EU TFTS unit; (b)	▪ Reduction in scale of minor terrorist activity = 20% ▪ Reduction in likelihood of a major terrorist attack = 35%

Policy Option	Costs	Benefits
	the central EU Agency will employ a slightly higher number of analysts as compared to B.1. The initial set-up costs of the system would be lower than B.1: 10% of the cost of software development and project management as it is assumed that UST would share know-how and expertise. The running costs are slightly lower as overheads and operational expenditure is slightly lower (lower number of Member States analysts placed at Europol)	
B.3.2 – EU TFTS extraction service	Costs are same as B1 except that (a) EU Central Unit extracts search results for Member States and analyses only for EU level bodies and third countries; (b) The Member States would be the only authorities to undertake the analysis of the searches	▪ Reduction in scale of minor terrorist activity = 15% ▪ Reduction in likelihood of a major terrorist attack = 30%
B.3.3 - Financial Intelligence Unit coordination service	The main difference in costs vis-a-vis B.1 relates to the creation of a new ad hoc body at EU level (FIU Platform)	▪ Reduction in scale of minor terrorist activity = 10% ▪ Reduction in likelihood of a major terrorist attack = 25%
B.4.1 - Data retention regime	Under this policy option, the DP would be required to retain the data on its server for a certain period. The option would eliminate the need to make requests for "raw" data and the related verification process. Searches would be run by DP on request of UST, Europol and/or MS. Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders. The cost of setting up and running the system at an EU level would be lower as: ▪ There would be no capital expenditure involved with the creation/ upgradation of a facility to house the system ▪ No costs associated with preparation or verification of request for data ▪ Lower number of FTE involved in running the system (18) The DP would be faced with higher staff costs. It is assumed that 4 staff would be recruited by the DP to run searches.	▪ Reduction in scale of minor terrorist activity = 10% ▪ Reduction in likelihood of a major terrorist attack = 25%
B.4.2 - Data retention regime and extraction mechanism	Costs are same as B4.1 except that 4 Europol analysts and 14 national analysts would be located on DP's premises or in a facility nearby	▪ Reduction in scale of minor terrorist activity = 10% ▪ Reduction in likelihood of a major terrorist attack = 25%
C.1 - Terrorism only	Same as B.3.1	▪ Same as B.3.1

Policy Option	Costs	Benefits
C.2 - Terrorism + serious organised crime	Same as B.3.1 except that there might be marginal additional costs associated with greater volumes of data being handled ▪ Reduction in scale of minor terrorist activity = 30% ▪ Reduction in likelihood of a major terrorist attack = 45% NB: includes the benefits of the preferred option concerning the structure, i.e. B.3.1	
D.1 - One Designated Provider	Same as B.3.1	▪ Same as B.3.1
D.2- Multiple Designated Providers	The cost to EU budget and national budgets are the same as B3.1. All costs accruing to DPs have been multiplied by 44 considering that the system would work with multiple Designated Providers and hence access, search and analyse FIN and other types of financial messages / other type of transaction data. The system will cover all ACH (42); SWIFT; and, PayPal	▪ Reduction in scale of minor terrorist activity = 30% ▪ Reduction in likelihood of a major terrorist attack = 45% NB: includes the benefits of the preferred option concerning the structure, i.e. B.3.1

IX.2 Annex 2 Table of costs

Incremental Costs of different Policy Options vis a vis Baseline Scenario

		EU Budget		MS Budget		Designated Provider(s)	
Option	Cost Category	Min	Max	Min	Max	Min	Max
Option A.1 (Baseline Scenario)	Initial Set-up Costs	0	0	0	0	0	0
	Running Costs (annual)	232,798	295,654			651,293	703,692
	Adminstrative Costs (annual)	40,370	70,330			15,354	15,354
Option A.2	Initial Set-up Costs	330,000	460,000	224,000	308,000	0	0
	Running Costs (annual)	407,397	344,541	2,208,085	2,415,855	0	0
	Adminstrative Costs (annual)	0	0	0	0	0	0
Option B.1	Initial Set-up Costs	8,124,591	10,437,804	0	0	455,800	708,000
	Running Costs (annual)	6,414,009	6,760,153	0	0	35,186	0
	Adminstrative Costs (annual)	5,820	8,730	0	0	0	0
Option B.2	Initial Set-up Costs	250,000	300,000	101,684,800	133,012,600	1,356,800	2,009,000
	Running Costs (annual)	-232,798	-295,654	62,990,812	68,086,812	46,701	11,515
	Adminstrative Costs (annual)	-40,370	-70,330	62,990,812	68,086,812	61,415	61,415
Option B.3(i)	Initial Set-up Costs	5,335,405	6,517,782	354,000	503,000	455,800	708,000
	Running Costs (annual)	6,114,394	6,459,538	1,960,837	2,168,607	35,186	0
	Adminstrative Costs (annual)	5,820	8,730	70,280	70,280	0	0
Option B.3(ii)	Initial Set-up Costs	5,335,405	6,517,782	354,000	503,000	455,800	708,000
	Running Costs (annual)	4,752,471	5,097,615	10,430,985	10,638,755	35,186	0
	Adminstrative Costs (annual)	5,820	8,730	70,280	70,280	0	0
Option B.3(iii)	Initial Set-up Costs	5,585,405	6,817,782	354,000	503,000	5,585,405	6,817,782
	Running Costs (annual)	5,436,829	5,781,973	21,894,728	22,232,498	5,018,333	5,373,934
	Adminstrative Costs (annual)	5,820	8,730	70,280	70,280	30,836	63,706
Option B.4(i)	Initial Set-up Costs	738,399	1,256,920	284,000	433,000	759,800	913,000
	Running Costs (annual)	1,632,095	1,578,840	1,680,837	1,748,607	955,086	909,724
	Adminstrative Costs (annual)	5,820	8,730	70,280	70,280	61,415	61,415
Option B.4(ii)	Initial Set-up Costs	2,209,869	2,947,246	354,000	503,000	755,000	907,000
	Running Costs (annual)	4,466,026	4,816,370	1,960,837	2,168,607	91,441	42,241
	Adminstrative Costs (annual)	5,820	8,730	70,280	70,280	61,415	61,415
Option D.2	Initial Set-up Costs	5,357,541	6,552,054	354,000	6,552,054	19,984,800	31,064,000
	Running Costs (annual)	6,114,394	6,459,538	1,960,837	6,755,192	28,005,610	30,258,768
	Adminstrative Costs (annual)	5,820	8,730	70,280	79,060	1,335,771	1,335,771

Overview of Costs of different Policy Options

		EU Budget		MS Budget		Designated Provider(s)	
Option	Cost Category	Min	Max	Min	Max	Min	Max
Option A.1 (Baseline Scenario)	Initial Set-up Costs	-	-	-	-	-	-
	Running Costs (annual)	232,798	295,654			651,293	703,692
	Adminstrative Costs (annual)	40,370	70,330			15,354	15,354
Option A.2	Initial Set-up Costs	330,000	460,000	224,000	308,000	-	-
	Running Costs (annual)	640,195	640,195	2,208,085	2,415,855	651,293	703,692
	Adminstrative Costs (annual)	40,370	70,330	-	-	15,354	15,354
Option B.1	Initial Set-up Costs	8,124,591	10,437,804	-	-	455,800	708,000
	Running Costs (annual)	6,646,807	7,055,807	-	-	686,479	703,692
	Adminstrative Costs (annual)	46,190	79,060	-	-	15,354	15,354
Option B.2	Initial Set-up Costs	250,000	300,000	101,684,800	133,012,600	1,356,800	2,009,000
	Running Costs (annual)	-	-	62,990,812	68,086,812	697,994	715,208
	Adminstrative Costs (annual)	-	-	62,990,812	68,086,812	76,768	76,768
Option B.3(i)	Initial Set-up Costs	5,335,405	6,517,782	354,000	503,000	455,800	708,000
	Running Costs (annual)	6,347,192	6,755,192	1,960,837	2,168,607	686,479	703,692
	Adminstrative Costs (annual)	46,190	79,060	70,280	70,280	15,354	15,354
Option B.3(ii)	Initial Set-up Costs	5,335,405	6,517,782	354,000	503,000	455,800	708,000
	Running Costs (annual)	4,985,269	5,393,269	10,430,985	10,638,755	686,479	703,692
	Adminstrative Costs (annual)	46,190	79,060	70,280	70,280	15,354	15,354
Option B.3(iii)	Initial Set-up Costs	5,585,405	6,817,782	354,000	503,000	5,585,405	6,817,782
	Running Costs (annual)	5,669,627	6,077,627	21,894,728	22,232,498	5,669,627	6,077,627
	Adminstrative Costs (annual)	46,190	79,060	70,280	70,280	46,190	79,060
Option B.4(i)	Initial Set-up Costs	738,399	1,256,920	284,000	433,000	759,800	913,000
	Running Costs (annual)	1,864,893	1,874,493	1,680,837	1,748,607	1,606,379	1,613,416
	Adminstrative Costs (annual)	46,190	79,060	70,280	70,280	76,768	76,768
Option B.4(ii)	Initial Set-up Costs	2,209,869	2,947,246	354,000	503,000	755,000	907,000
	Running Costs (annual)	4,698,824	5,112,024	1,960,837	2,168,607	742,735	745,933
	Adminstrative Costs (annual)	46,190	79,060	70,280	70,280	76,768	76,768
Option D.2	Initial Set-up Costs	5,357,541	6,552,054	354,000	6,552,054	19,984,800	31,064,000
	Running Costs (annual)	6,347,192	6,755,192	1,960,837	6,755,192	28,656,903	30,962,460
	Adminstrative Costs (annual)	46,190	79,060	70,280	79,060	1,351,124	1,351,124

IT Costs

	Labour			Purchase of equipment					Travel			Total	
	Days	*Daily Rate*	*Cost*	*Units*	*Per Unit Cost- min*	*Per Unit Cost- max*	*Cost - min*	*Cost - max*	*Units*	*Per Unit Cost*	*Cost*	*MIN*	MAX
Develop Functional Specifications	30	€ 2,500	€ 75,000					€ 0	5	€ 1,000	€ 5,000	€ 80,000	€ 150,000
Develop System Architecture	30	€ 2,500	€ 75,000					€ 0	5	€ 1,000	€ 5,000	€ 80,000	€ 150,000
Develop Preliminary Design Specification	30	€ 2,500	€ 75,000					€ 0	5	€ 1,000	€ 5,000	€ 80,000	€ 150,000
Develop Detailed Design Specifications	60	€ 2,500	€ 150,000					€ 0	5	€ 1,000	€ 5,000	€ 155,000	€ 300,000
Develop Acceptance Test Plan	20	€ 2,500	€ 50,000					€ 0	5	€ 1,000	€ 5,000	€ 55,000	€ 150,000
Development of full technical specification	170		€ 425,000	0				€ 0	25		€ 25,000	€ 450,000	€ 900,000
Installation of dedicated/ secure data lines (T1 variant)	1	€ 2,500	€ 2,500						1	€ 1,000	€ 1,000	€ 3,500	€ 3,500
Main Database Server	1	€ 2,500	€ 2,500	1	€ 40,000	€ 50,000	€ 40,000	€ 50,000				€ 43,500	€ 53,500
Application Server	1	€ 2,500	€ 2,500	1	€ 40,000	€ 50,000	€ 40,000	€ 50,000	1	€ 1,000	€ 1,000	€ 42,500	€ 52,500
On-Line Analytical Processing (OLAP) Server	1	€ 2,500	€ 2,500	1	€ 40,000	€ 50,000	€ 40,000	€ 50,000				€ 42,500	€ 52,500
Network Server	1	€ 2,500	€ 2,500	1	€ 40,000	€ 50,000	€ 40,000	€ 50,000				€ 42,500	€ 52,500
Backup and Restore (BAR)	1	€ 2,500	€ 2,500	1	€ 40,000	€ 50,000	€ 40,000	€ 50,000	1	€ 1,000	€ 1,000	€ 43,500	€ 53,500
SAN Device	1	€ 2,500	€ 2,500	1	€ 100,000	€ 25,000	€ 100,000	€ 25,000	1	€ 1,000	€ 1,000	€ 103,500	€ 28,500
Analysts terminal	1	€ 2,500	€ 2,500	10	€ 1,000	€ 2,000	€ 10,000	€ 20,000	1	€ 1,000	€ 1,000	€ 13,500	€ 23,500
Overseer terminal				2	€ 1,000	€ 2,000	€ 2,000	€ 4,000				€ 2,000	€ 4,000
Procurement and installation of hardware	8		€ 20,000	18			€ 312,000	€ 299,000	5		€ 5,000	€ 337,000	€ 324,000
Purchase of software and licences:													
Firewall				1	€ 20,000	€ 100,000	€ 20,000	€ 100,000				€ 20,000	€ 100,000
Oracle				1	€ 500,000	€ 750,000	€ 500,000	€ 750,000				€ 500,000	€ 750,000
ETL Software (data extraction software)				1	€ 350,000	€ 500,000	€ 350,000	€ 500,000				€ 350,000	€ 500,000
OLAP Reporting Tool				1	€ 350,000	€ 500,000	€ 350,000	€ 500,000				€ 350,000	€ 500,000
Other software				1	€ 500,000	€ 750,000	€ 500,000	€ 750,000				€ 500,000	€ 750,000
Develop bespoke Software - entity extraction tool				1	€ 750,000	€ 1,000,000	€ 750,000	€ 1,000,000				€ 750,000	€ 1,000,000
Perform Acceptance Test	20	€ 2,500	€ 50,000						0		€ 0	€ 50,000	€ 50,000
Perform Post Project Review	20	€ 2,500	€ 50,000						0		€ 0	€ 50,000	€ 50,000
Software development	40		€ 100,000	6			€ 2,470,000	€ 3,600,000	0		€ 0	€ 2,570,000	€ 3,700,000
Customer Progress Meetings/Reports	20	€ 2,500	€ 50,000						5	€ 1,000	€ 5,000	€ 55,000	€ 55,000
Internal Status Meetings/Reports	20	€ 2,500	€ 50,000						5	€ 1,000	€ 5,000	€ 55,000	€ 55,000
Third-Party Vendor Interface	15	€ 2,500	€ 37,500						5	€ 1,000	€ 5,000	€ 42,500	€ 42,500
Configuration Management	15	€ 2,500	€ 37,500						5	€ 1,000	€ 5,000	€ 42,500	€ 42,500
Quality Assurance	10	€ 2,500	€ 25,000						5	€ 1,000	€ 5,000	€ 30,000	€ 30,000
Project Management:	80		€ 200,000	0				€ 0	25		€ 25,000	€ 225,000	€ 225,000
Contingency (10%)												€ 313,200	€ 424,900

Online Analytical Processing, a category of software tools that provides analysis of data stored in a database. OLAP tools enable users to analyze different dimensions of multidimensional data. For example, it provides time series and trend analysis views. OLAP often is used in data mining.

The chief component of OLAP is the OLAP server, which sits between a client and a database management systems (DBMS). The OLAP server understands how data is organized in the database and has special functions for analyzing the data. There are OLAP servers available for nearly all the major database systems.

HR Costs

EU Budget	Assumption	Average Staff Costs (Daily)	Average Staff Costs (annual)	A2		B1		B3.1		B3.2		B3.3		B.4.1		B.4.2	
Function/ Role				No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost
Preparation of requests for raw	AD-10	€ 582	€ 128,039			1	€ 128,039	1	€ 128,039	1	€ 128,039	1	€ 128,039				
Supervision of all operations	AD-14	€ 954	€ 209,827			1	€ 209,827	1	€ 209,827	1	€ 209,827	1	€ 209,827	1	€ 209,827	1	€ 128,039
Programme Management Team	AD-14	€ 954	€ 209,827			3	€ 629,481	2	€ 419,654	2	€ 419,654	3	€ 629,481			2	€ 419,654
Dedicated Technicians/ IT Staff	AD-7	€ 402	€ 88,400			4	€ 353,600	4	€ 353,600	4	€ 353,600	4	€ 353,600			4	€ 839,308
External communication	AD-7	€ 402	€ 88,400			1	€ 88,400	1	€ 88,400	1	€ 88,400	1	€ 88,400	1	€ 88,400	1	€ 88,400
Security agents	Average Agent cost of EUR 57,600 (source: IA IT Agency)	€ 262	€ 57,600			2	€ 115,200	3	€ 172,800	3	€ 172,800	2	€ 115,200				€ 0
Independent Overseer	AD-10	€ 582	€ 128,039	1	€ 128,039	1	€ 128,039	1	€ 128,039	1	€ 128,039	1	€ 128,039	1	€ 128,039	1	€ 57,600
External Auditors	AD-10	€ 582	€ 128,039			2	€ 256,078	2	€ 256,078	2	€ 256,078	2	€ 256,078	2	€ 256,078	2	€ 256,078
TFTS Analysts	AD-10	€ 582	€ 128,039	4	€ 512,156	10	€ 1,280,389	8	€ 1,024,311	4	€ 512,156		€ 0	4	€ 512,156	4	€ 512,156
Legal Officer	AD-8	€ 455	€ 100,019			1	€ 100,019	1	€ 100,019	1	€ 100,019	1	€ 100,019	1	€ 100,019	1	€ 128,039
Data Protection Officer	AD-8	€ 455	€ 100,019			2	€ 200,038	2	€ 200,038	1	€ 100,019	2	€ 200,038	1	€ 100,019	1	€ 100,019
Verification and authorisation of	AD-12	€ 745	€ 163,909			2	€ 327,817	2	€ 327,817	1	€ 163,909	2	€ 327,817				
				5	€ 640,195	30	€ 3,816,927	28	€ 3,408,622	22	€	20	€	11	€ 1,394,537	17	€ 2,529,292

National Budget	Assumption	Average Staff Costs (Daily)	Average Staff Costs (annual)	A2		B1		B3.1		B3.2		B3.3		D1		D2	
Function/ Role				No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost
Preparation of requests for raw	AD-10	€ 502	€ 110,378			1	€ 110,378	0	€ 0	0	€ 0	0	€ 0				
Supervision of all operations	AD-14	€ 822	€ 180,885			1	€ 180,885	0	€ 0	14	€	27	€				
Programme Management Team	AD-14	€ 822	€ 180,885			3	€ 542,656	0	€ 0	14	€	27	€				
Dedicated Technicians/ IT Staff	AD-7	€ 346	€ 76,207			4	€ 304,828	0	€ 0	0	€ 0	0	€ 0				
External communication	AD-7	€ 346	€ 76,207			1	€ 76,207	0	€ 0	0	€ 0	0	€ 0				
Security agents	Average Agent cost of EUR 57,600 (source: IA IT Agency)	€ 262	€ 57,600			2	€ 115,200	0	€ 0	0	€ 0	0	€ 0				
Independent Overseer	AD-10	€ 502	€ 110,378			1	€ 110,378	0	€ 0	0	€ 0	0	€ 0				
External Auditors	AD-10	€ 502	€ 110,378			2	€ 220,757	0	€ 0	0	€ 0	0	€ 0				
TFTS Analysts	AD-10	€ 502	€ 110,378			10	€ 1,103,784	14	€ 1,545,297	14	€	27	€	14	€ 1,545,297	14	€ 1,545,297
Legal Officer	AD-8	€ 392	€ 86,223			1	€ 86,223	0	€ 0	14	€	27	€				
Data Protection Officer	AD-8	€ 392	€ 86,223			2	€ 172,446	0	€ 0	14	€	27	€				
Verification and authorisation of	AD-12	€ 642	€ 141,300			2	€ 282,601	0	€ 0	14	€	27	€				
				0	€ 0	30	€ 3,306,344	14	€ 1,545,297	84	€	162	€	14	€ 1,545,297	14	€ 1,545,297

Designated Provider

Function/ Role	Assumption	Average Staff Costs (Daily)	Average Staff Costs (annual)	No. of FTE	Cost	No. of FTE	Cost	No. of FTE	Cost
Overseers	see below	€ 640	€ 140,742	3	€ 422,226	3	€ 422,226	3	€ 422,226
Staff involved in preparing and transmitting data	see below	€ 640	€ 140,742	0.25	€ 35,186	1	€ 140,742	1	€ 140,742
Legal advisor + training	see below	€ 640	€ 140,742	0.25	€ 35,186	0.5	€ 70,371	0.5	€ 70,371
External auditor	see below	€ 640	€ 140,742	0.25	€ 35,186	0.5	€ 70,371	0.5	€ 70,371
Staff involved in conducting searches	see below	€ 640	€ 140,742	0	€ 0	6	€ 844,453	0	€ 0
				3.75	€ 527,783	11	€ 1,548,163	5	€ 703,711

SWIFT Staff Costs	2010	2009
Payroll and related charges	254,321,000	270,206,000
No. of employees	1,807	
Average staff costs - Annual	140,742	
Average Staff Costs - Daily	640	

http://www.swift.com/about_swift/publications/annual_reports/annual_review_2010/SWIFT_AR2010_financial_statements.pdf
http://www.swift.com/about_swift/publications/annual_reports/annual_review_2010/SWIFT_AR2010.pdf

European Commission: Monthly Basic Salary (2010) and Adjustments

Grade	Seniority Step I	II	III	IV	V	Monthly - Average	Annual salary	+ Expat Allowance	2011 prices	2012 prices	Daily rate	MS Salary (minus expat allowance)	Daily rate
16	16,919	17,630	18,371			17,640	211,680	245,548	252,915	260,502	1,184	224,571	1,021
15	19,534	15,582	16,237	16,688	16,919	16,992	203,904	236,528	243,624	250,933	1,141	216,321	983
14	13,216	13,772	14,351	14,750	14,954	14,208	170,502	197,782	203,715	209,827	954	180,885	822
13	11,681	12,172	12,684	13,036	13,216	12,558	150,695	174,806	180,050	185,452	843	159,872	727
12	10,324	10,758	11,210	11,522	11,681	11,099	133,189	154,499	159,134	163,909	745	141,300	642
11	9,125	9,508	9,908	10,184	10,324	9,810	117,717	136,552	140,648	144,868	658	124,886	568
10	8,065	8,404	8,757	9,001	9,125	8,670	104,042	120,689	124,310	128,039	582	110,378	502
9	7,128	7,428	7,740	7,955	8,065	7,663	91,956	106,669	109,869	113,165	514	97,556	443
8	6,300	6,565	6,841	7,031	7,128	6,773	81,274	94,277	97,106	100,019	455	86,223	392
7	5,568	5,802	6,046	6,214	6,300	5,986	71,832	83,326	85,825	88,400	402	76,207	346
6	4,921	5,128	5,344	5,492	5,568	5,291	63,488	73,646	75,855	78,131	355	67,354	306
5	4,350	4,532	4,723	4,854	4,921	4,676	56,113	65,091	67,043	69,055	314	59,530	271
4	3,844	4,006	4,174	4,290	4,350	4,133	49,594	57,529	59,255	61,033	277	52,614	239
3	3,398	3,541	3,689	3,792	3,844	3,653	43,833	50,846	52,372	53,943	245	46,502	211
2	3,003	3,129	3,261	3,351	3,398	3,228	38,741	44,940	46,288	47,676	217	41,100	187
1	2,654	2,766	2,882	2,962	3,003	2,853	34,241	39,719	40,911	42,138	192	36,326	165

Annual Inflation 3%

Source: http://ec.europa.eu/civil_service/docs/salary_officials_en.pdf

Notes:

Each grade is broken up into five seniority steps . Basic salaries are adjusted annually in line with inflation and purchasing power in the EU countries

Staff who have left home country to come and work for the European Commission, are entitled to an expatriation allowance equivalent to 16% of basic salary.

Officials accumulate 1.9% pension rights every year

A.1 Cost Estimates

Note: This policy option involves no further/ new action being taken by the EU. Under this option, the present arrangements as per the US-EU TFTP Agreement would continue

Budget	Cost Category	Cost Heading	Cost Item	Per Unit Costs	No. of Units	No. of days per year	Cost	Per Unit Costs	No. of Units	No. of days per year	Cost	Explanatory Comments
EU Budget	Running costs	Verfication and authorisation of UST requests	Europol analysts' time (AD-10)	582.00	3	48	83,807	582	3	72	125,711	2 to 3 days per month X 3 Analysts
		Initiating/ coordinating requests for searches / process 'leads' through pontaneous provision of information	Europol analysts' time (AD-10)	582.00	3	12	20,952	582	3	24	41,904	1 to 2 days per month X 3 Analysts
		Independent EU Overseer	Salary costs	582.00	1	220	128,039	582	1	220	128,039	1 FTE (AD10 equivalent)
			sub-total				**232,798**				**295,654**	
	Administrative Costs	Independent Review of EU-TFTS	Time spent on review	582.00	5	5	14,550	582	5	10	29,100	5 to 10 days X 5 reviewers
			Reimbursable expenses	500.00	5	5	12,500	500	5	10	25,000	5 to 10 days X EUR 500 per day
			Travel	1,500.00	5		7,500	1,500	5		7,500	EUR 1,500 per person
		Monitoring and reporting by the European Commission	Staff time	582.00	1	10	5,820	582	1	15	8,730	10 to 15 days X 1 EC staff (AD10)
			sub-total				**40,370**				**70,330**	
DP	Running costs (annual)	HR costs	Staff costs	640	3.75	220	527,783	640	3.75	220	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)				100,000				150,000	Guesstimate
			Staff training	640	3.75	5	11,995	640	3.75	6	14,394	6 FTE X 5 to 6 days a year X Daily labour costs (EUR 674). Daily wage = annual staff costs (EUR 148 298) divided by 220 working days.
		Overheads	Management costs	960	1	12	11,515	960	1	12	11,515	1 day of management time per month: 12 days per year X daily wage (EUR 670 + 50%)
			sub-total				**651,293**				**703,692**	
	Administrative Costs	Record keeping	Record keeping	640	2	12	15,354	640	2	12	15,354	2 staff X 2 days per month X Daily wages
			sub-total				**15,354**				**15,354**	

A.2 Cost Estimates

Note: Costs essential relate to Europol relocating its analysts to UST and 14 Member States locating analysts to UST

				Range of Costs (EUR)		
Budget	Cost Category	Cost Heading	Cost Item	Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Relocation of EU Analysts	Relocation of Analysts to UST	80,000	160,000	EUR 20,000 to EUR 40,000 X 4 analyst
			sub-total	**330,000**	**460,000**	
	Running Costs (annual)	HR costs	Staff costs	512,156	512,156	4 FTE analysts
			Independent EU overseer	128,039	128,039	See HR Costs
			sub-total	**640,195**	**640,195**	
	Administrative Costs		Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**40,370**	**70,330**	
MS	Initial Set-up Costs	HR costs	Initial expenditure for relocation of national analysts at EU unit	210,000	280,000	EUR 15,000 to 20,000 per Member State X 14 Member States
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**224,000**	**308,000**	
	Running Costs (annual)	HR costs	Staff costs	1,792,545	1,792,545	No. of TFTS analysts (14) X EUR 128,039
		Operational expenditure	Operational expenditure e.g. T&S, travel	280,000	420,000	No. of TFTS Analysts X EUR 20,000 to 30,000
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**2,208,085**	**2,415,855**	
DP	Running costs (annual)	HR costs	Staff costs	527,783	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)	100,000	150,000	
			Staff training	11,995	14,394	3.75 FTE X 5 to 6 days a year X Daily labour costs
		Overheads	Management costs	11,515	11,515	1 day of management time per month: 12 days per year X daily wage (EUR 670 + 50%)
			sub-total	**651,293**	**703,692**	
	Administrative Costs	Information Obligations	Record keeping and reporting	15,354	15,354	2 staff X 2 days per month X Daily wages
			sub-total	**15,354**	**15,354**	

B1 Cost Estimates

Budget	Cost Category	Cost Heading	Cost Item	Range of Costs (EUR) Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Secure facility to house the TFTS	*option a* - Capital expenditure for new facility	3,150,000	3,600,000	Based on rough average cost of EUR 7000 to EUR 8000 per 1m2 for constructing a central facility, a back-up facility and office space, which are serviced and equipped (source: based on figures for construction of a UK data centre, 15 August 2007 www.datacenterjournal.com which were used in IA of IT Agency). The total floor space required for the TFTP is assumed to be 100m2 plus additional 350 m2 for accommodating 7 additional analysts (source: space requirements are based on a guesstimate)
			option b - Upgradation of existing facility	787,500	900,000	Assumed to be 1/4th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	337,000	324,000	See sheet IT costs
			Software development	2,570,000	3,700,000	See sheet IT costs
			Project management	225,000	225,000	See sheet IT costs
			Contingency (10%)	313,200	424,900	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	7,136	14,272	10 analysts X 1 to 2 days X EUR 582 plus 2 trainers X 1 to 2 days X 658
			Recruitment costs	15,000	20,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**8,124,591**	**10,437,804**	
	Running Costs (annual)	Human Resources	Preparation of requests for data and coordination with DPs	128,039	128,039	See HR costs sheet
			Supervision of all operations	209,827	209,827	See HR costs sheet
			Programme Management Team	629,481	629,481	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	353,600	353,600	See HR costs sheet
			External communication	88,400	88,400	See HR costs sheet
			Security agents	115,200	115,200	See HR costs sheet
			Independent Overseer	128,039	128,039	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			TFTS Analysts	1,280,389	1,280,389	See HR costs sheet
			Legal Officer	100,019	100,019	See HR costs sheet
			Data Protection Officer	200,038	200,038	See HR costs sheet
			Verification and validation of requests	327,817	327,817	See HR costs sheet
		Operating costs of the system	Hardware maintenance	200,000	250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			Vendor support	100,000	200,000	Guesstimate
			Software maintenance, updates & licenses	1,000,000	1,250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			T1 data lines	6,000	12,000	500 to 1000 per month
		Other costs	Security clearance of new staff	12,000	15,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	448,890	448,890	No. of FTE X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	1,062,990	1,062,990	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**6,646,807**	**7,055,807**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports by centralised agency	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Internal organisation	Adapting/setting up systems and processes to comply with the legislation	100,000	200,000	
		IT costs	Data extraction system	100,000	200,000	
		HR costs	Security clearance of staff	4,800	6,000	6 X EUR 800 to 1000 per person;
			Initial staff training	1,000	2,000	
			sub-total	**455,800**	**708,000**	
	Running costs (annual)	HR costs	Staff costs	562,968	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)	100,000	150,000	
			Staff training	11,995	14,394	3.75 FTE X 5 to 6 days a year X Daily labour costs
		Overheads	Management costs	11,515	11,515	1 day of management time per month: 12 days per year X daily wage (EUR 670 + 50%)
			sub-total	**686,479**	**703,692**	
	Administrative Costs	Information Obligations	Record keeping and reporting	15,354	15,354	2 staff X 2 days per month X Daily wages
			sub-total	**15,354**	**15,354**	

B2 Cost Estimates

Note: This option is based on the assumption that 14 Member State will develop a national system. As such most costs have been multiplied by 14

Budget	Cost Category	Cost Heading	Cost Item	Range of Costs (EUR) Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
MS	Initial Set-up Costs	Development of national legislative instrument	Development of legal framework for national TFTS	2,800,000	4,200,000	200,000 to 300,000 per Member State
		Development of full technical specification	Procurement of external IT consultancy	6,300,000	12,600,000	See sheet IT costs
		Secure facility to house the TFTS	*option a* - Capital expenditure for new facility	35,280,000	40,320,000	Costs assumed to be 80% of the costs of a central unit at EU level on basis that national systems will be accessing less data
			option b - Upgradation of existing facility	8,820,000	10,080,000	Assumed to be 1/4th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	4,718,000	4,536,000	See sheet IT costs
			Software development	35,980,000	51,800,000	See sheet IT costs. It is assumed that UST will assist so costs reduced by 2/3rds
			Project management	3,150,000	3,150,000	See sheet IT costs. It is assumed that UST will assist so costs reduced by 2/3rds
			Contingency (10%)	4,384,800	5,948,600	See sheet IT costs
		Other costs	Development of training and certification	252,000	378,000	3 trainers X 10 to 15 days X EUR 600 per day X 14 Member States
			Initial training of analysts	86,800	173,600	10 analysts X 1 to 2 days X EUR 500 plus 2 trainers X 1 to 2 days X EUR 600 X 14 Member States
			Recruitment costs	210,000	280,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**101,684,800**	**133,012,600**	
	Running Costs (annual)	Human Resources	Preparation of requests for data and coordination with DPs	1,545,297	1,545,297	See HR costs sheet
			Supervision of all operations	2,532,394	2,532,394	See HR costs sheet
			Programme Management Team	7,597,181	7,597,181	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	4,267,589	4,267,589	See HR costs sheet
			External communication	1,066,897	1,066,897	See HR costs sheet
			Security agents	1,612,800	1,612,800	See HR costs sheet
			Independent Overseer	1,545,297	1,545,297	See HR costs sheet
			External Auditors	3,090,595	3,090,595	See HR costs sheet
			TFTS Analysts	15,452,973	15,452,973	See HR costs sheet
			Legal Officer	1,207,125	1,207,125	See HR costs sheet
			Data Protection Officer	2,414,251	2,414,251	See HR costs sheet
			Verification and validation of requests	3,956,413	3,956,413	See HR costs sheet
		Operating costs of the system	Hardware maintenance	2,800,000	3,500,000	EUR 200,000 to EUR 250,000 X 14 Member States
			Vendor support	1,400,000	2,800,000	EUR 100,000 to EUR 200,000 X 14 Member States
			Software maintenance, updates & licenses	7,000,000	8,400,000	EUR 500,000 to EUR 600,000 X 14 Member States
			T1 data lines	84,000	168,000	500 to 1000 per month
		Other costs	Security clearance of new staff	168,000	210,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	2,100,000	2,520,000	No. of FTE X EUR 10,000 to EUR 12,000 X 14 Member States
			Operational expenditure	3,150,000	4,200,000	No. of FTE X EUR 15,000 to EUR 20,000 X 14 Member States
			sub-total	**62,990,812**	**68,086,812**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	455,700	455,700	5 Member review team X 5 to 10 working days X daily labour cost of EUR 502 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports by TFTS agency	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**596,260**	**596,260**	
DP	Initial Set-up Costs	Legal costs Internal organisation IT costs HR costs	Familiarising with the new legislation and planning how to comply	1,050,000	1,400,000	EUR 75,000 to 100,000 per Member State
			Adapting/setting up systems and processes to comply with the legislation	200,000	400,000	
			Data extraction system	100,000	200,000	
			Security clearance of staff	4,800	6,000	6 X EUR 800 to 1000 per person;
			Initial staff training	2,000	3,000	
			sub-total	**1,356,800**	**2,009,000**	
	Running costs (annual)	HR costs	Staff costs	562,968	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)	100,000	150,000	
			Staff training	11,995	14,394	3.75 FTE X 5 to 6 days a year X Daily labour costs
		Overheads	Management costs	23,031	23,031	2 days of management time per month: 24days per year X daily wage (EUR 670 + 50%)
			sub-total	**697,994**	**715,208**	
	Administrative Costs	Information Obligations	Record keeping and reporting	76,768	76,768	2 staff X 5 days per month X EUR 674
			sub-total	**76,768**	**76,768**	

B3.1 Cost Estimates

Note: Costs are same as B1 except that (a) Member States can now request the central EU Agency to conduct searches on their behalf Member States could opt to either request searches to be run on their behalf by the central unit (having to substantiate their requests for searches or undertake their own searches, through designated national TFTS analysts which would be based in the same location as the EU TFTS unit; (b) the central EU Agency will employ a slightly higher number of analysts as compared to B1

				Range of Costs (EUR)		
Budget	Cost Category	Cost Heading	Cost Item	Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Secure facility to house the TFTS	*option a* - Capital expenditure for new facility	3,150,000	3,600,000	Based on rough average cost of EUR 7000 to EUR 8000 per 1m2 for constructing a central facility, a back-up facility and office space, which are serviced and equipped (source: based on figures for construction of a UK data centre, 15 August 2007 www.datacenterjournal.com which were used in IA of IT Agency). The total floor space required for the TFTP is assumed to be 100m2 plus additional 350 m2 for accommodating 7 additional analysts (source: space requirements are based on a guesstimate)
			option b - Upgradation of existing facility	787,500	900,000	Assumed to be 1/4th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	337,000	324,000	See sheet IT costs
			Software development	257,000	370,000	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Project management	22,500	22,500	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Contingency (10%)	61,650	71,650	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	7,136	14,272	No. of analysts X 1 to 2 days X EUR 582 plus 2 trainers X 1 to 2 days X 658
			Recruitment costs	15,000	20,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**5,335,405**	**6,517,782**	
	Running Costs (annual)	Human Resources	Preparation of requests for data and coordination with DPs	128,039	128,039	See HR costs sheet
			Supervision of all operations	209,827	209,827	See HR costs sheet
			Programme Management Team	419,654	419,654	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	353,600	353,600	See HR costs sheet
			External communication	88,400	88,400	See HR costs sheet
			Security agents	172,800	172,800	See HR costs sheet
			Independent Overseer	128,039	128,039	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			TFTS Analysts	1,024,311	1,024,311	See HR costs sheet
			Legal Officer	100,019	100,019	See HR costs sheet
			Data Protection Officer	200,038	200,038	See HR costs sheet
			Verification and validation of requests	327,817	327,817	See HR costs sheet
		Operating costs of the system	Hardware maintenance	200,000	250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			Vendor support	100,000	200,000	Guesstimate
			Software maintenance, updates & licenses	1,000,000	1,250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			T1 data lines	6,000	12,000	500 to 1000 per month
		Other costs	Security clearance of new staff	12,000	14,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	628,446	628,446	(No. of FTE + No. of national analysts located at EU central unit) X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	992,124	992,124	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**6,347,192**	**6,755,192**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports by centralised agency	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Internal organisation	Adapting/setting up systems and processes to comply with the legislation	100,000	200,000	
		IT costs	Data extraction system	100,000	200,000	
		HR costs	Security clearance of staff	4,800	6,000	6 X EUR 800 to 1000 per person;
			Initial staff training	1,000	2,000	
			sub-total	**455,800**	**708,000**	
	Running costs (annual)	HR costs	Staff costs	562,968	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)	100,000	150,000	
			Staff training	11,995	14,394	3.75 FTE X 5 to 6 days a year X Daily labour costs (EUR 640)
		Overheads	Management costs	11,515	11,515	1 day of management time per month: 12 days per year X daily wage (EUR 640 + 50%)
			sub-total	**686,479**	**703,692**	
	Administrative Costs	Information Obligations	Record keeping and reporting	15,354	15,354	2 staff X 2 days per month X EUR 640
			sub-total	**15,354**	**15,354**	
MS	Initial Set-up Costs	Legal costs	Setting up protocols for coordination with EU unit	130,000	195,000	EUR 10,000 to 14,000 per Member State X 13 Member States who don't designate national TFTP analysts at central EU Unit
		HR costs	Initial expenditure for relocation of national analysts at EU unit	210,000	280,000	EUR 15,000 to 20,000 per Member State X 14 Member States
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**354,000**	**503,000**	
	Running Costs (annual)	HR costs	Staff costs	1,545,297	1,545,297	
		Operational expenditure	Operational expenditure e.g. T&S, travel	280,000	420,000	No. of TFTS Analysts X EUR 20,000 to 30,000
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**1,960,837**	**2,168,607**	
	Administrative	Information Obligations	Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**70,280**	**70,280**	

B3.2 Cost Estimates

Note: Costs are same as B1 except that (a) EU Central Unit extracts search results for Member States and analyses only for EU level bodies and third countries; (b) The Member States would be the only authorities to undertake the analysis of the searches

Budget	Cost Category	Cost Heading	Cost Item	Range of Costs (EUR) Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Secure facility to house the TFTS	*option a* - Capital expenditure for new facility	3,150,000	3,600,000	Based on rough average cost of EUR 7000 to EUR 8000 per 1m2 for constructing a central facility, a back-up facility and office space, which are serviced and equipped (source: based on figures for construction of a UK data centre, 15 August 2007 www.datacenterjournal.com which were used in IA of IT Agency). The total floor space required for the TFTP is assumed to be 100m2 plus additional 350 m2 for accommodating 7 additional analysts (source: space requirements are based on a guesstimate)
			option b - Upgradation of existing facility	787,500	900,000	Assumed to be 1/4 th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	337,000	324,000	See sheet IT costs
			Software development	257,000	370,000	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Project management	22,500	22,500	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Contingency (10%)	61,650	71,650	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	3,644	7,288	No. of analysts X 1 to 2 days X EUR 582 plus 2 trainers X 1 to 2 days X 658
			Recruitment costs	15,000	20,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**5,335,405**	**6,517,782**	
	Running Costs (annual)	Human Resources	Preparation of requests for data and coordination with DPs	128,039	128,039	See HR costs sheet
			Supervision of all operations	209,827	209,827	See HR costs sheet
			Programme Management Team	419,654	419,654	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	353,600	353,600	See HR costs sheet
			External communication	88,400	88,400	See HR costs sheet
			Security agents	172,800	172,800	See HR costs sheet
			Independent Overseer	128,039	128,039	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			TFTS Analysts	512,156	512,156	See HR costs sheet
			Legal Officer	100,019	100,019	See HR costs sheet
			Data Protection Officer	100,019	100,019	See HR costs sheet
			Verification and validation of requests	163,909	163,909	See HR costs sheet
		Operating costs of the system	Hardware maintenance	200,000	250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			Vendor support	100,000	200,000	Guesstimate
			Software maintenance, updates & licenses	1,000,000	1,250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			T1 data lines	6,000	12,000	500 to 1000 per month
		Other costs	Security clearance of new staff	12,000	14,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	538,668	538,668	(No. of FTE + No. of national analysts located at EU central unit) X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	496,062	496,062	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**4,985,269**	**5,393,269**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports by centralised agency	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Internal organisation	Adapting/setting up systems and processes to comply with the legislation	100,000	200,000	
		IT costs	Data extraction system	100,000	200,000	
		HR costs	Security clearance of staff	4,800	6,000	6 X EUR 800 to 1000 per person;
			Initial staff training	1,000	2,000	
			sub-total	**455,800**	**708,000**	
	Running costs (annual)	HR costs	Staff costs	562,968	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)	100,000	150,000	
			Staff training	11,995	14,394	3.75 FTE X 5 to 6 days a year X Daily labour costs (EUR 640)
		Overheads	Management costs	11,515	11,515	1 day of management time per month: 12 days per year X daily wage (EUR 640 + 50%)
			sub-total	**686,479**	**703,692**	
	Administrative Costs	Information Obligations	Record keeping and reporting	15,354	15,354	2 staff X 2 days per month X EUR 640
			sub-total	**15,354**	**15,354**	
MS	Initial Set-up Costs	Legal costs	Setting up protocols for coordination with EU unit	130,000	195,000	EUR 10,000 to 14,000 per Member State X 13 Member States who don't designate national TFTP analysts at central EU Unit
		HR costs	Initial expenditure for relocation of national analysts at EU unit	210,000	280,000	EUR 15,000 to 20,000 per Member State X 14 Member States
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**354,000**	**503,000**	
	Running Costs (annual)	HR costs	Supervision of all operations	1,545,297	1,545,297	See HR costs
			Management of operations	2,532,394	2,532,394	See HR costs
			TFTS Analysts	1,545,297	1,545,297	See HR costs
			Legal Officers	1,207,125	1,207,125	See HR costs
			DPOs	1,207,125	1,207,125	See HR costs
			Verification and authorisation of requests	1,978,206	1,978,206	See HR costs
		Operational expenditure	Operational expenditure e.g. T&S, travel	280,000	420,000	No. of TFTS Analysts X EUR 20,000 to 30,000
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**10,430,985**	**10,638,755**	
	Administrative	Information Obligations	Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**70,280**	**70,280**	

B3.3 Cost Estimates

Note: The main difference in costs relates to the creation of a new ad hoc body at EU level (FIU Platform)

Budget	Cost Category	Cost Heading	Cost Item	Range of Costs (EUR) Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice to set up legislative framework for TFTS	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
			Legislative framework for new ad hoc body at EU level	250,000	300,000	As above
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Secure facility to house the TFTS	*option a* - Capital expenditure for new facility	3,150,000	3,600,000	Based on rough average cost of EUR 7000 to EUR 8000 per 1m2 for constructing a central facility, a back-up facility and office space, which are serviced and equipped (source: based on figures for construction of a UK data centre, 15 August 2007 www.datacenterjournal.com which were used in IA of IT Agency). The total floor space required for the TFTP is assumed to be 100m2 plus additional 350 m2 for accommodating 7 additional analysts (source: space requirements are based on a guesstimate)
			option b - Upgradation of existing facility	787,500	900,000	Assumed to be 1/4th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	337,000	324,000	See sheet IT costs
			Software development	257,000	370,000	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Project management	22,500	22,500	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Contingency (10%)	61,650	71,650	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	7,136	14,272	No. of analysts X 1 to 2 days X EUR 502 plus 2 trainers X 1 to 2 days X 658
			sub-total	**5,585,405**	**6,817,782**	
	Running Costs (annual)	Human Resources	Preparation of requests for data and coordination with DPs	128,039	128,039	See HR costs sheet
			Supervision of all operations	209,827	209,827	See HR costs sheet
			Programme Management Team	629,481	629,481	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	353,600	353,600	See HR costs sheet
			External communication	88,400	88,400	See HR costs sheet
			Security agents	115,200	115,200	See HR costs sheet
			Independent Overseer	128,039	128,039	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			Legal Officer	100,019	100,019	See HR costs sheet
			Data Protection Officer	200,038	200,038	See HR costs sheet
			Verification and validation of requests	327,817	327,817	See HR costs sheet
		Operating costs of the system	Hardware maintenance	200,000	250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			Vendor support	100,000	200,000	Guesstimate
			Software maintenance, updates & licenses	1,000,000	1,250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			T1 data lines	6,000	12,000	500 to 1000 per month
		Other costs	Security clearance of new staff	12,000	14,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	822,965	822,965	No. of FTE X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	992,124	992,124	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**5,669,627**	**6,077,627**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports by centralised agency	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Internal organisation	Adapting/setting up systems and processes to comply with the legislation	100,000	200,000	
		IT costs	Data extraction system	100,000	200,000	
		HR costs	Security clearance of staff	4,800	6,000	6 X EUR 800 to 1000 per person;
			Initial staff training	1,000	2,000	
			sub-total	**455,800**	**708,000**	
	Running costs (annual)	HR costs	Staff costs	562,968	527,783	See HR costs
		Operational costs	Technical updates (software and hardware)	100,000	150,000	
			Staff training	11,995	14,394	3.75 FTE X 5 to 6 days a year X Daily labour costs (EUR 640).
		Overheads	Management costs	11,515	11,515	1 day of management time per month: 12 days per year X daily wage (EUR 640 + 50%)
			sub-total	**686,479**	**703,692**	
	Administrative Costs	Information Obligations	Record keeping and reporting	15,354	15,354	2 staff X 2 days per month X EUR 640
			sub-total	**15,354**	**15,354**	
MS	Initial Set-up Costs	Legal costs	Setting up protocols for coordination with EU unit	130,000	195,000	EUR 10,000 to 14,000 per Member State X 13 Member States who don't designate national TFTP analysts at central EU Unit
		HR costs	Initial expenditure for relocation of national analysts at EU unit	210,000	280,000	EUR 15,000 to 20,000 per Member State X 14 Member States
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**354,000**	**503,000**	
	Running Costs (annual)	HR costs	Supervision of all operations	4,883,902	4,883,902	See HR costs
			Management of operations	4,883,902	4,883,902	See HR costs
			TFTS Analysts	2,980,216	2,980,216	See HR costs
			Legal Officers	2,328,027	2,328,027	See HR costs
			DPOs	2,328,027	2,328,027	See HR costs
			Verification and authorisation of requests	3,815,112	3,815,112	See HR costs
		Operational expenditure	Operational expenditure e.g. T&S, travel	540,000	810,000	No. of TFTS Analysts X EUR 20,000 to 30,000
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**21,894,728**	**22,232,498**	
	Administrative	Information Obligations	Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**70,280**	**70,280**	

B4.1 Cost Estimates

Budget	Cost Category	Cost Heading	Cost Item	Range of Costs (EUR) Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	3,644	7,288	No. of analysts X 1 to 2 days X EUR 582 plus 2 trainers X 1 to 2 days X 658
			Recruitment costs	15,000	20,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**738,399**	**1,256,920**	
	Running Costs (annual)	Human Resources	Supervision of all operations	209,827	209,827	See HR costs sheet
			Independent Overseer	128,039	128,039	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			TFTS Analysts	512,156	512,156	See HR costs sheet
			Legal Officer	100,019	100,019	See HR costs sheet
			Data Protection Officer	100,019	100,019	See HR costs sheet
		Other costs	Security clearance of new staff	4,400	14,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	164,593	164,593	(No. of FTE + No. of national analysts located at EU central unit) X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	389,763	389,763	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**1,864,893**	**1,874,493**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Internal organisation HR costs	Adapting/setting up systems and processes to comply with the legislation	500,000	600,000	
			Security clearance of staff	8,800	11,000	€800 to €1000 per person;
			Initial staff training	1,000	2,000	
			sub-total	**759,800**	**913,000**	
	Running costs (annual)	HR costs	Staff costs	1,548,163	1,548,163	See HR costs
			Staff training	35,186	42,223	No. of FTE X 5 to 6 days a year X Daily labour costs (EUR 640)
		Overheads	Management costs	23,031	23,031	2 day of management time per month: 24 days per year X daily wage (EUR 640 + 50%)
			sub-total	**1,606,379**	**1,613,416**	
	Administrative Costs	Information Obligations	Record keeping and reporting	76,768	76,768	2 staff X 5 days per month X EUR 640
			sub-total	**76,768**	**76,768**	
MS	Initial Set-up Costs	Legal costs	Setting up protocols for coordination with DPs	270,000	405,000	EUR 1000 to 2000 per Member State
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**284,000**	**433,000**	
	Running Costs (annual)	HR costs	Staff costs	1,545,297	1,545,297	
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**1,680,837**	**1,748,607**	
	Administrative	Information Obligations	Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**70,280**	**70,280**	

B4.2 Cost Estimates

Note: Costs are same as B4.1 except that analysts are actually located on DP's premises

Budget	Cost Category	Cost Heading	Cost Item	Range of Costs (EUR) Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Secure facility to house the TFTS	Upgradation of existing facility	787,500	900,000	Assumed to be 1/4 th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	337,000	324,000	See sheet IT costs
			Software development	257,000	370,000	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Project management	22,500	22,500	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Contingency (10%)	61,650	71,650	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	9,464	9,464	No. of analysts X 1 to 2 days X EUR 582 plus 2 trainers X 1 to 2 days X 658
			Recruitment costs	15,000	20,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**2,209,869**	**2,947,246**	
	Running Costs (annual)	Human Resources	Supervision of all operations	128,039	128,039	See HR costs sheet
			Programme Management Team	419,654	419,654	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	839,308	839,308	See HR costs sheet
			External communication	88,400	88,400	See HR costs sheet
			Independent Overseer	57,600	57,600	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			TFTS Analysts	512,156	512,156	See HR costs sheet
			Legal Officer	128,039	128,039	See HR costs sheet
			Data Protection Officer	100,019	100,019	See HR costs sheet
		Operating costs of the system	Hardware maintenance	200,000	250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			Vendor support	100,000	200,000	Guesstimate
			Software maintenance, updates & licenses	1,000,000	1,250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			T1 data lines	6,000	12,000	500 to 1000 per month
		Other costs	Security clearance of new staff	6,800	14,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	254,371	254,371	(No. of FTE + No. of national analysts located at EU central unit) X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	602,361	602,361	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**4,698,824**	**5,112,024**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Internal organisation	Adapting/setting up systems and processes to comply with the legislation	500,000	600,000	
		HR costs	Security clearance of staff	4,000	5,000	No. of staff X1000 per person
			Initial staff training	1,000	2,000	
			sub-total	**755,000**	**907,000**	
	Running costs (annual)	HR costs	Staff costs	703,711	703,711	See HR costs
			Staff training	15,993	19,192	No. of FTE X 5 to 6 days a year X Daily labour costs (EUR 640)
		Overheads	Management costs	23,031	23,031	2 day of management time per month: 24 days per year X daily wage (EUR 640 + 50%)
			sub-total	**742,735**	**745,933**	
	Administrative Costs	Information Obligations	Record keeping and reporting	76,768	76,768	2 staff X 5 days per month X EUR 640
			sub-total	**76,768**	**76,768**	
MS	Initial Set-up Costs	Legal costs	Setting up protocols for coordination with DPs	130,000	195,000	EUR 1000 to 2000 per Member State
		HR costs	Initial expenditure for relocation of national analysts at EU unit	210,000	280,000	EUR 15,000 to 20,000 per analyst
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**354,000**	**503,000**	
	Running Costs (annual)	HR costs	Staff costs	1,545,297	1,545,297	
		Operational expenditure	Operational expenditure e.g. T&S, travel	280,000	420,000	No. of TFTS Analysts X EUR 20,000 to 30,000
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**1,960,837**	**2,168,607**	
	Administrative	Information Obligations	Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**70,280**	**70,280**	

D2 Cost Estimates

Note: The costs are same as B3.1 except that the system would work with multiple Designated Providers and hence access, search and analyse FIN and other types of financial messages / other type of transaction data. The system will cover all ACH (42); SWIFT; and, PayPal

Budget	Cost Category	Cost Heading	Cost Item	Min	Max	Explanatory comments
EU	Initial Set-up Costs	Development of EU legislative instrument	Procurement of external legal advice	250,000	300,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses
		Development of full technical specification	Procurement of external IT consultancy	450,000	900,000	See sheet IT costs
		Secure facility to house the TFTS	*option a* - Capital expenditure for new facility	3,150,000	3,600,000	Based on rough average cost of EUR 7000 to EUR 8000 per 1m2 for constructing a central facility, a back-up facility and office space, which are serviced and equipped (source: based on figures for construction of a UK data centre, 15 August 2007 www.datacenterjournal.com which were used in IA of IT Agency). The total floor space required for the TFTP is assumed to be 100m2 plus additional 350 m2 for accommodating 7 additional analysts (source: space requirements are based on a guesstimate)
			option b - Upgradation of existing facility	787,500	900,000	Assumed to be 1/4th cost of new build
		Development of IT infrastructure	Hardware procurement and installation	337,000	324,000	See sheet IT costs
			Software development	257,000	370,000	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Project management	22,500	22,500	See sheet IT costs. It is assumed that UST will assist so costs reduced to 10%
			Contingency (10%)	61,650	71,650	See sheet IT costs
		Other costs	Development of training and certification	19,755	29,632	3 AD11 staff X 10 to 15 days each
			Initial training of analysts	7,136	14,272	No. of analysts X 1 to 2 days X EUR 582 plus 2 trainers X 1 to 2 days X 658
			Recruitment costs	15,000	20,000	Launching a call for candidates, selection process etc. Figure based on a guesstimate
			sub-total	**5,357,541**	**6,552,054**	
	Running Costs (annual)	Human Resources	Preparation of requests for data and coordination with DPs	128,039	128,039	See HR costs sheet
			Supervision of all operations	209,827	209,827	See HR costs sheet
			Programme Management Team	419,654	419,654	See HR costs sheet
			Dedicated Technicians/ IT Staff (24/7 availability and back up)	353,600	353,600	See HR costs sheet
			External communication	88,400	88,400	See HR costs sheet
			Security agents	172,800	172,800	See HR costs sheet
			Independent Overseer	128,039	128,039	See HR costs sheet
			External Auditors	256,078	256,078	See HR costs sheet
			TFTS Analysts	1,024,311	1,024,311	See HR costs sheet
			Legal Officer	100,019	100,019	See HR costs sheet
			Data Protection Officer	200,038	200,038	See HR costs sheet
			Verification and validation of requests	327,817	327,817	See HR costs sheet
		Operating costs of the system	Hardware maintenance	200,000	250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			Vendor support	100,000	200,000	Guesstimate
			Software maintenance, updates & licenses	1,000,000	1,250,000	Based on IT Agency IA and US Feasibility Study of cross border electronic funds transfer system
			T1 data lines	6,000	12,000	500 to 1000 per month
		Other costs	Security clearance of new staff	12,000	14,000	€800 to €1000 per person; half the persons require clearance on an annual basis
			Overheads and other admin expenditure	628,446	628,446	(No. of FTE + No. of national analysts located at EU central unit) X EUR 14,963 (Europol's overheads per FTE)
			Operational expenditure	992,124	992,124	No. of FTE X EUR 35,433 (Europol's operational expenditure per FTE)
			sub-total	**6,347,192**	**6,755,192**	
	Administrative Costs	Independent Review	Independent Review of EU-TFTS	34,550	61,600	5 Member review team X 5 to 10 working days X daily labour cost of EUR 582 (AD-10). Plus reimbursable expenses (EUR 500 per person per day) and travel (EUR 1,500 X 5)
		Information Obligations	Preparation of reports by centralised agency	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			EC monitoring and reporting	5,820	8,730	10 to 15 days X daily labour cost of EUR 582 (AD-10).
			sub-total	**46,190**	**79,060**	
DP*	Initial Set-up Costs	Legal costs	Familiarising with the new legislation and planning how to comply	11,000,000	13,200,000	Educated guess: 2,500 per day X 90 to 100 days legal input + 25,000 to 50,000 expenses X 44 DPs
		Internal organisation	Adapting/setting up systems and processes to comply with the legislation	4,400,000	8,800,000	EUR 100,000 to 200,000 X 44 DPs
		IT costs	Data extraction system	4,400,000	8,800,000	EUR 100,000 to 200,000 X 44 DPs
		HR costs	Security clearance of staff	140,800	176,000	4 X EUR 800 to 1000 per person X 44 DPs
			Initial staff training	44,000	88,000	EUR 1,000 to 2,000 X 44DPs
			sub-total	**19,984,800**	**31,064,000**	
	Running costs (annual)	HR costs	Staff costs	23,222,449	23,222,449	See HR costs X 44 DPs
		Operational costs	Technical updates (software and hardware)	4,400,000	6,600,000	EUR 100,000 to 150,000 X 44 DPs
			Staff training	527,783	633,340	3.75 FTE X 5 to 6 days a year X Daily labour costs (EUR 640) X 44 DPs
		Overheads	Management costs	506,672	506,672	1 day of management time per month: 12 days per year X daily wage (EUR 640 + 50%) X 44 DPs
			sub-total	**28,656,903**	**30,962,460**	
	Administrative Costs	Information Obligations	Record keeping and reporting	1,351,124	1,351,124	2 staff X 2 days per month X EUR 640 X 44 DPs
			sub-total	**1,351,124**	**1,351,124**	
MS	Initial Set-up Costs	Legal costs	Setting up protocols for coordination with EU unit	130,000	195,000	EUR 10,000 to 14,000 per Member State X 13 Member States who don't designate national TFTP analysts at central EU Unit
		HR costs	Initial expenditure for relocation of national analysts at EU unit	210,000	280,000	EUR 15,000 to 20,000 per Member State X 14 Member States
			Initial staff training	14,000	28,000	EUR 1000 to 2000 per analyst
			sub-total	**354,000**	**503,000**	
	Running Costs (annual)	HR costs	Staff costs	1,545,297	1,545,297	
		Operational expenditure	Operational expenditure e.g. T&S, travel	280,000	420,000	No. of TFTS Analysts X EUR 20,000 to 30,000
			Issuing regular guidance and updates	135,540	203,310	10 to 15 days X daily labour cost of EUR 502 (AD-10) X 27 Member States
			sub-total	**1,960,837**	**2,168,607**	
	Administrative	Information Obligations	Monitoring and reporting by national civil service	70,280	70,280	10 to 15 days X daily labour cost of EUR 502 (AD-10).
			sub-total	**70,280**	**70,280**	

*Costs have been multiplied by 44